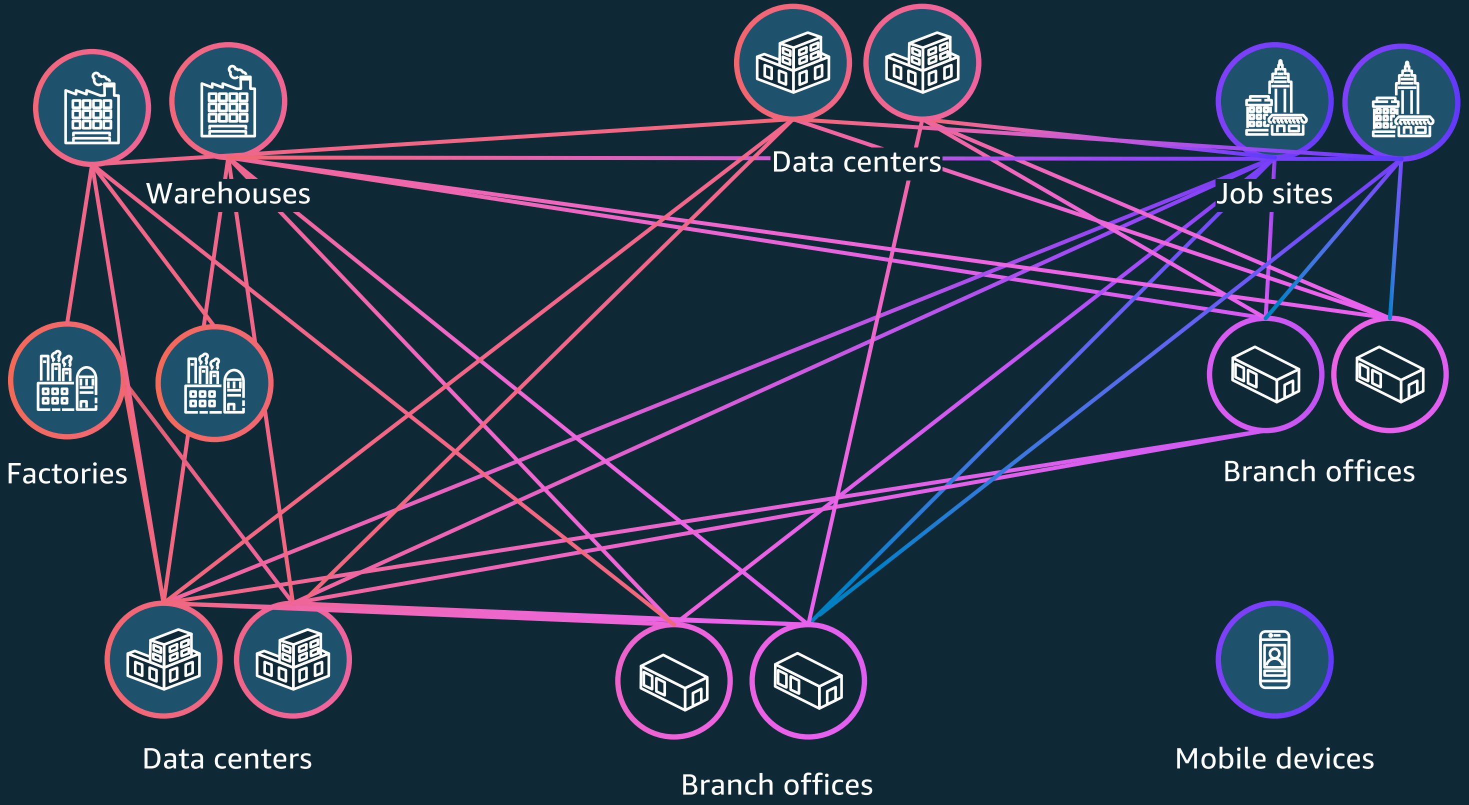
AWS Networking

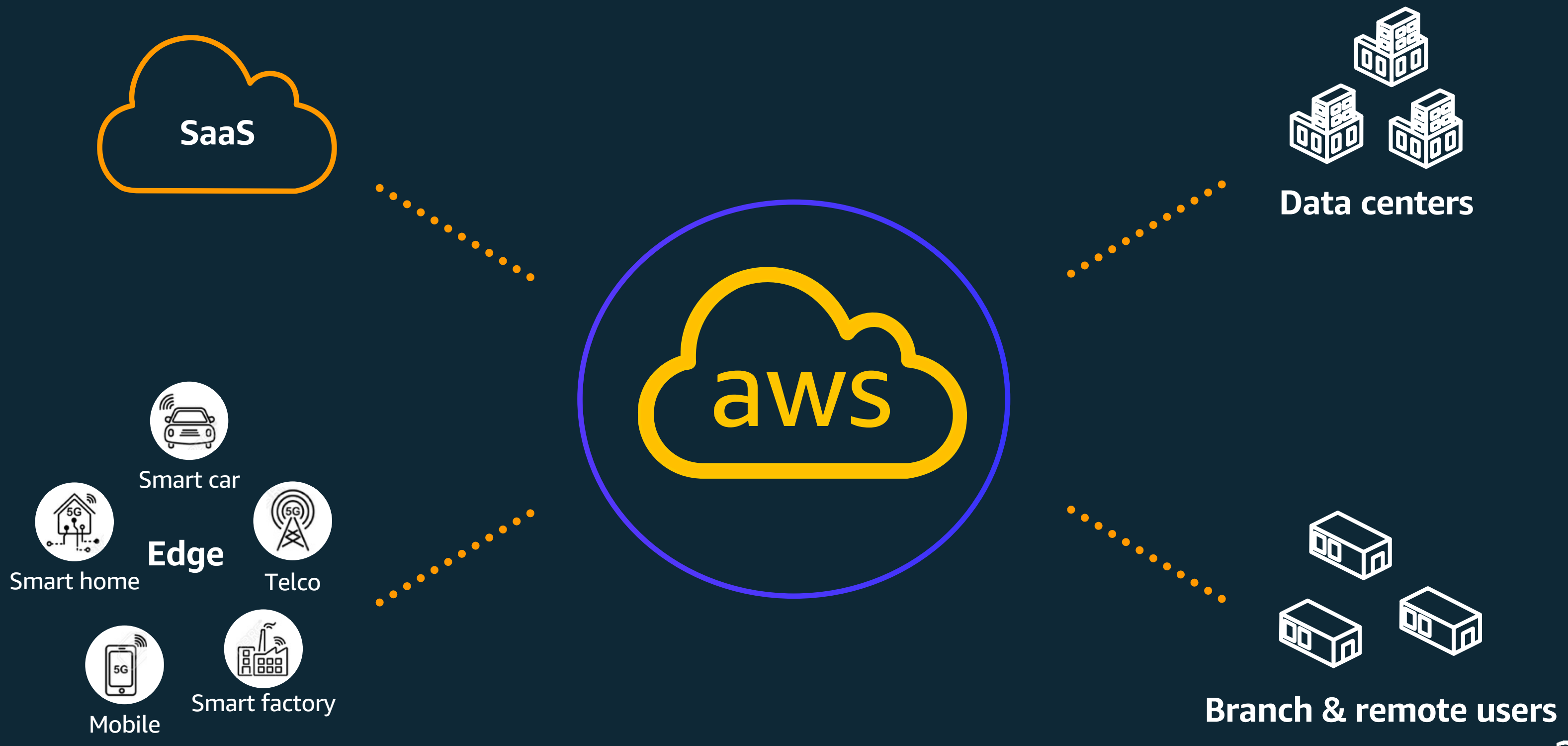
Networking to make your cloud journey easier

Networking is Complex



AWS Networking Vision

FROM THE EDGE TO THE DATA CENTER



AWS Networking Tenets

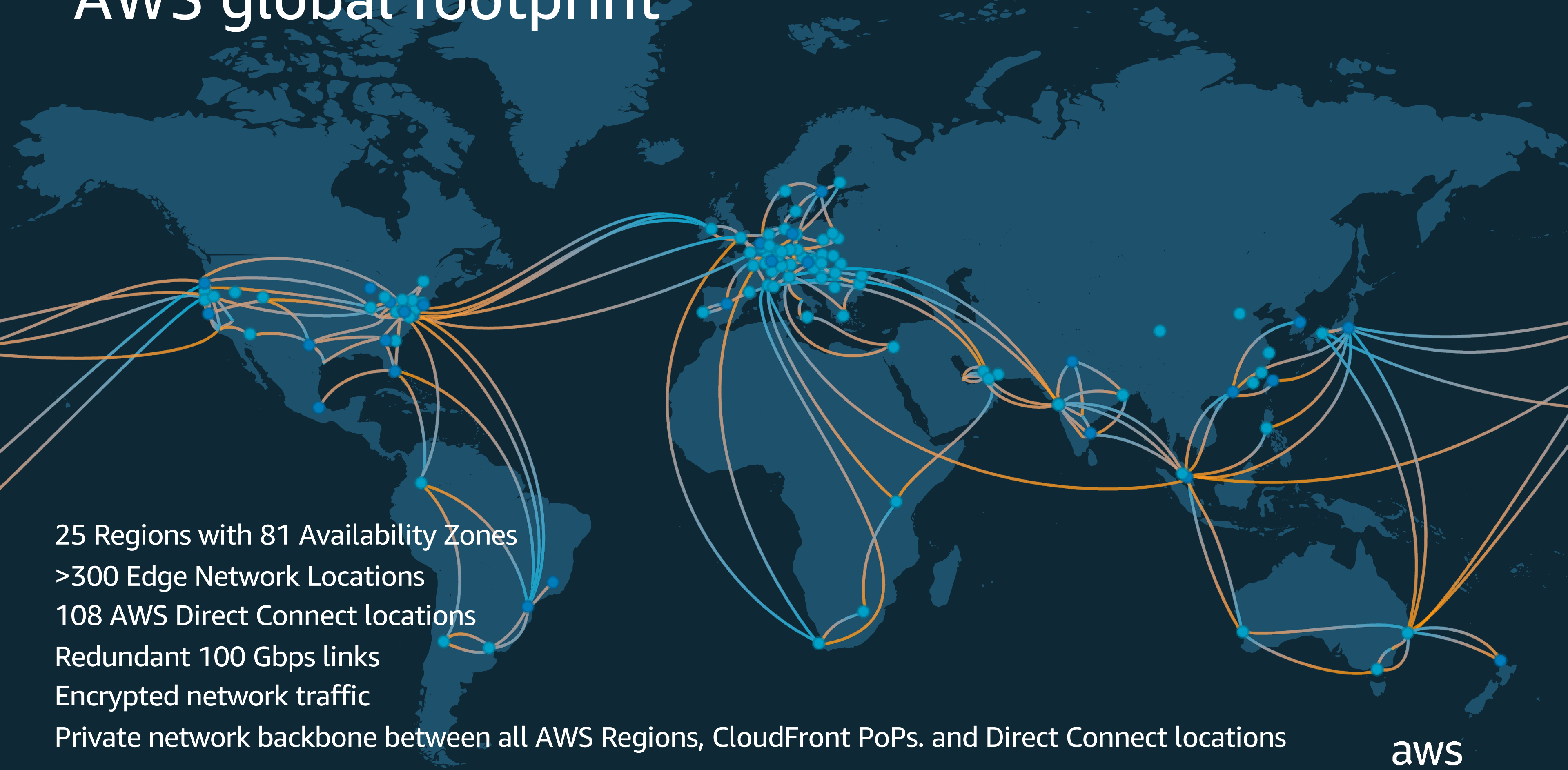
User Experience within AWS cloud and beyond

- Easier to secure and scale
- Abstract network complexity
- Seamless hybrid cloud network
- Centralized manageability and visibility

Operational Excellence

- Secure
- Available
- Scalable
- Performant

AWS global footprint



25 Regions with 81 Availability Zones

>300 Edge Network Locations

108 AWS Direct Connect locations

Redundant 100 Gbps links

Encrypted network traffic

Private network backbone between all AWS Regions, CloudFront PoPs. and Direct Connect locations

aws

Why have a global network?

Security

Traffic traverses our infrastructure rather than the internet

Availability

Controlling scaling and redundancy

Reliable performance

Controlling paths customer traffic traverses

Connecting closer to customers

Avoiding internet “hot spots” or sub-optimal external connectivity

All region-to-region traffic traverses the global network*

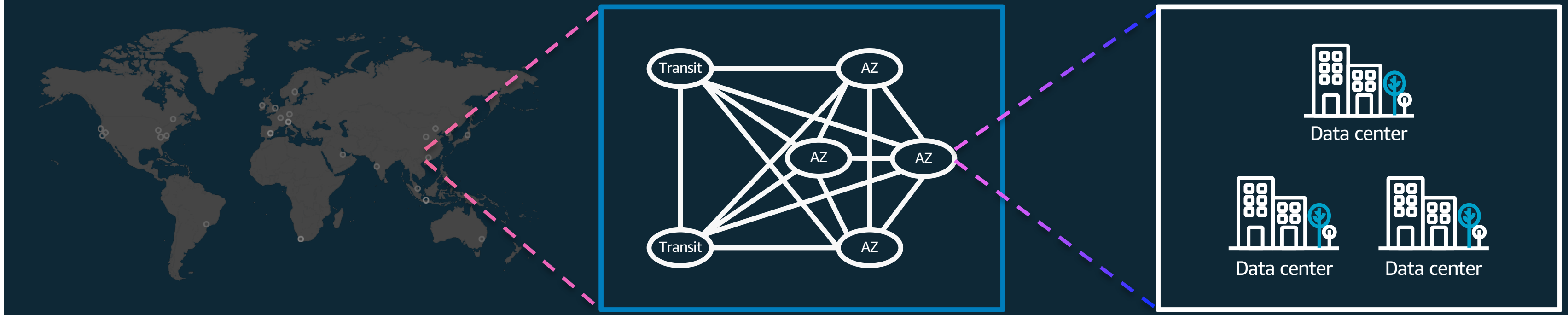
*except within the People’s Republic of China

Fault tolerance in our physical infrastructure

AWS Regions are comprised of multiple AZs for high availability and scalability

AWS Region

AWS Availability Zone (AZ)



Each Region has two independent, fully redundant transit centers to connect to the global network

Each Availability Zone consists of one or more data centers and has independent power, networking, and connectivity

Regional network availability

Dark Fiber Spans

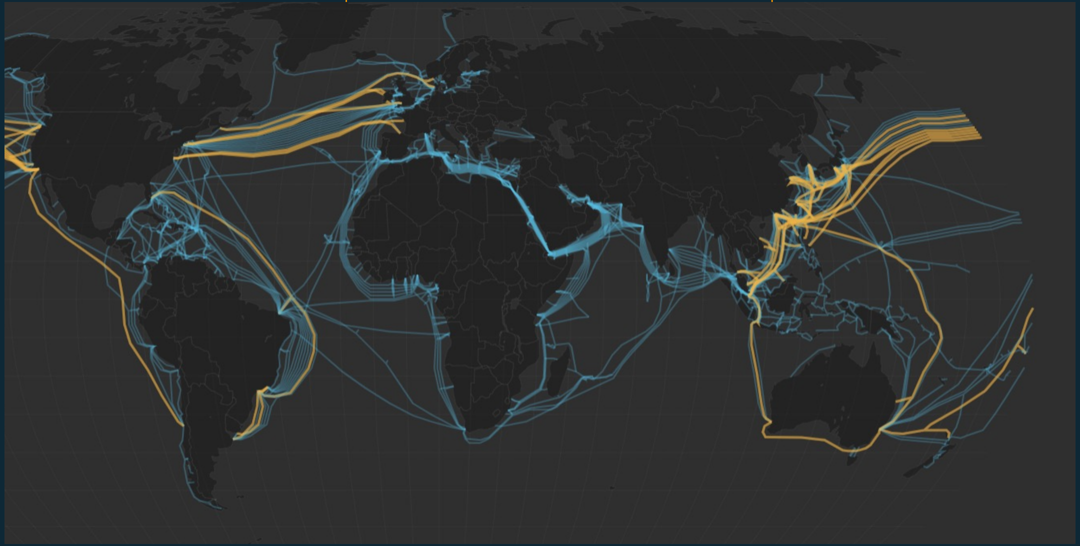
Optimized for low latency and physical diversity

Amazon Controlled

Regularly inspect the routes that fibers follow

Location Tracking

Geospatial coordinates are used to track the location of fiber cables



Virtual Private Cloud (VPC)

VPC

Virtual Private Cloud

Provision a logically isolated cloud where you can launch AWS resources into a virtual network

Security Groups & ACLs

NAT Gateway

Flow Logs

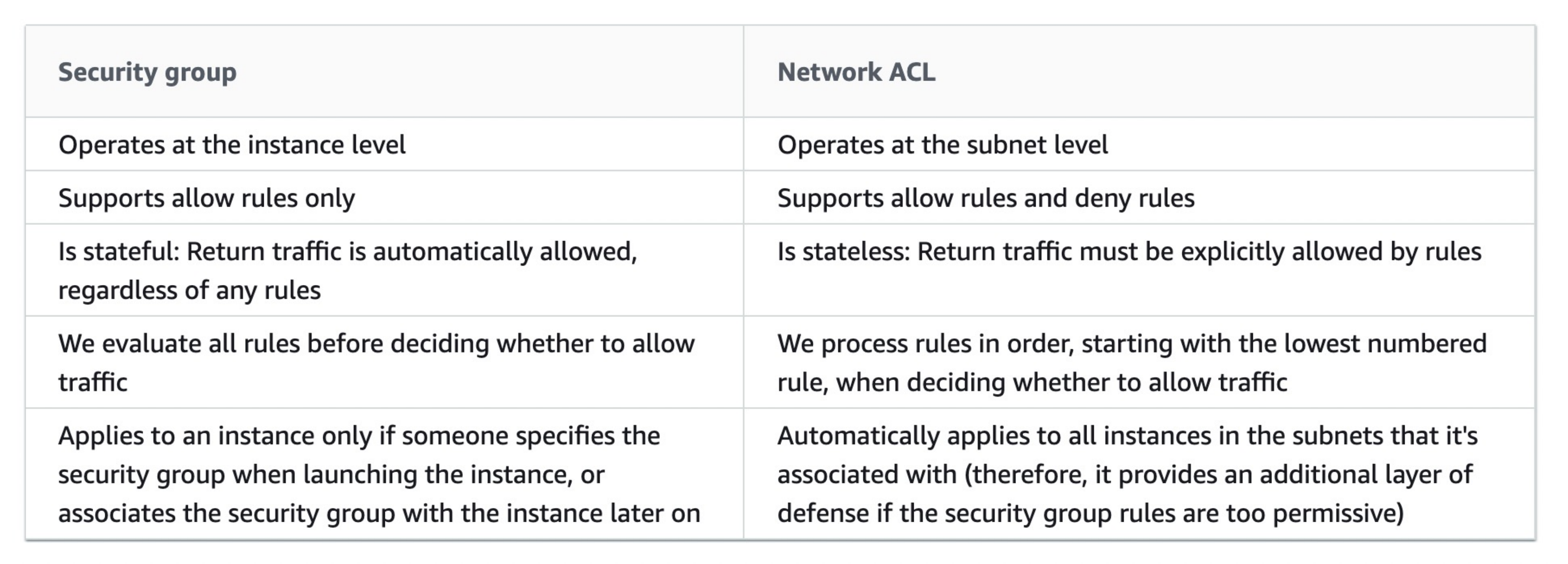
VPC Endpoints

Private and secure connectivity to Amazon S3 and Amazon DynamoDB

Amazon S3

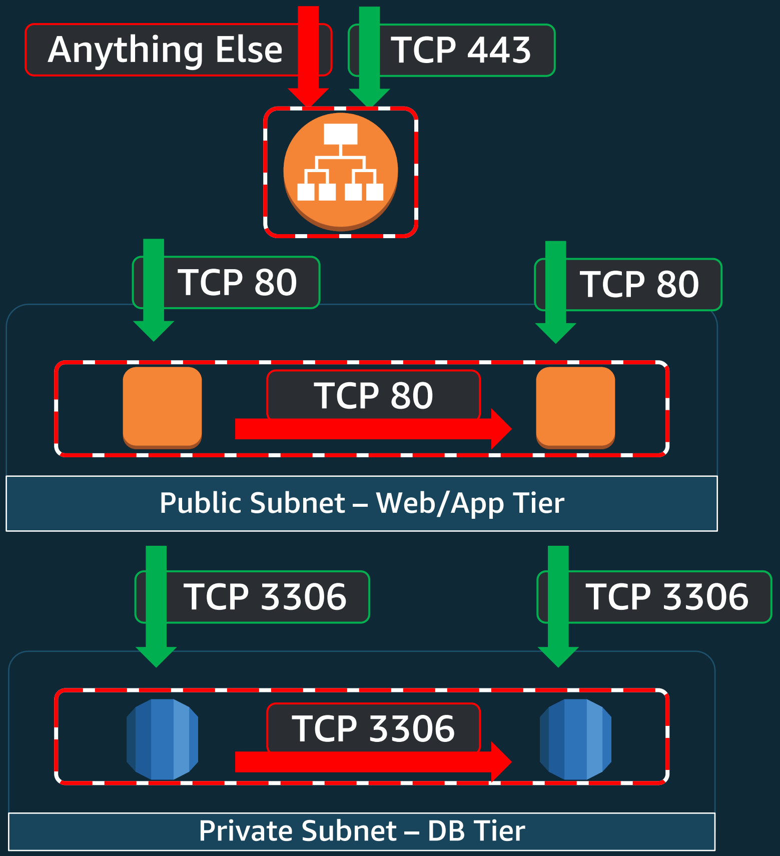
Amazon DynamoDB

Security Groups and Network ACLs

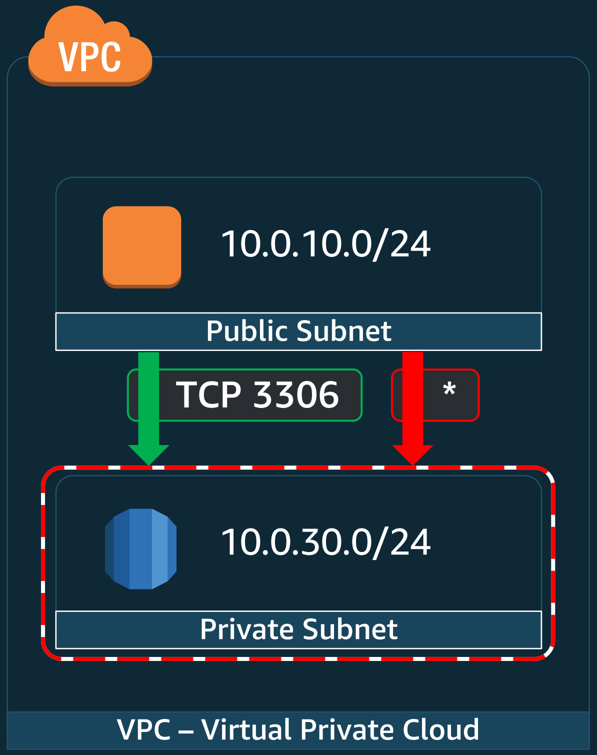


Security group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in order, starting with the lowest numbered rule, when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets that it's associated with (therefore, it provides an additional layer of defense if the security group rules are too permissive)

Security Groups



NACLs



Route tables

- Route tables contain rules for which packets go where
- Your VPC has a *default* route table
- But, you can create and assign different route tables to different subnets

Internet Gateway

- An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.
- It is bi-directional
- An internet gateway serves two purposes: to provide a target in your VPC route tables for internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses. For more information, see Enable internet access.
- An internet gateway supports IPv4 and IPv6 traffic. It does not cause availability risks or bandwidth constraints on your network traffic. There's no additional charge for having an internet gateway in your account.

NAT Gateway

- A NAT gateway is a Network Address Translation (NAT) service.
- It is one-directional
- You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.
- Public NAT Gateway: for instances in private subnet to connect to the Internet
- Private NAT Gateway: for instances in private subnet to connect to other VPCs and on-premises. Internet connection is blocked.

Customer and Virtual Private Gateway

- Customer Gateway aka CGW = customer side of a connection between AWS and customer’s data center/on-premises

- Virtual Private Gateway = AWS side of a connection between AWS and customer’s data center/on-premises

VPC Endpoint

- A VPC endpoint enables connections between a virtual private cloud (VPC) and supported services, without requiring that you use an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Therefore, your VPC is not exposed to the public internet.

- VPC endpoints are virtual devices. They are horizontally scaled, redundant, and highly available VPC components.

AWS Direct Connect

Benefits

Dedicated private connection from on-premised to AWS

Consistent network performance

Compatible with all AWS services

Reduced bandwidth costs

Key capabilities

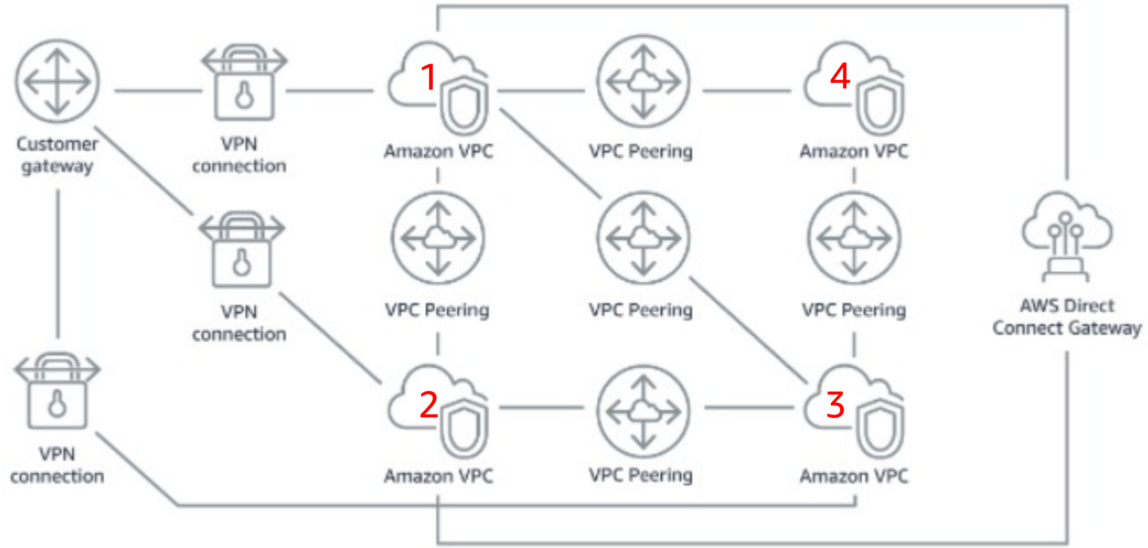
>100 Direct Connect locations globally

>50 Direct Connect delivery partners

Connect to any AWS Region from any location with Direct Connect Gateway

Integration with VMware Cloud on AWS

VPC Peering



Complexity increases with scale. You must maintain routing tables within each VPC and connect to each onsite location using separate network gateways.

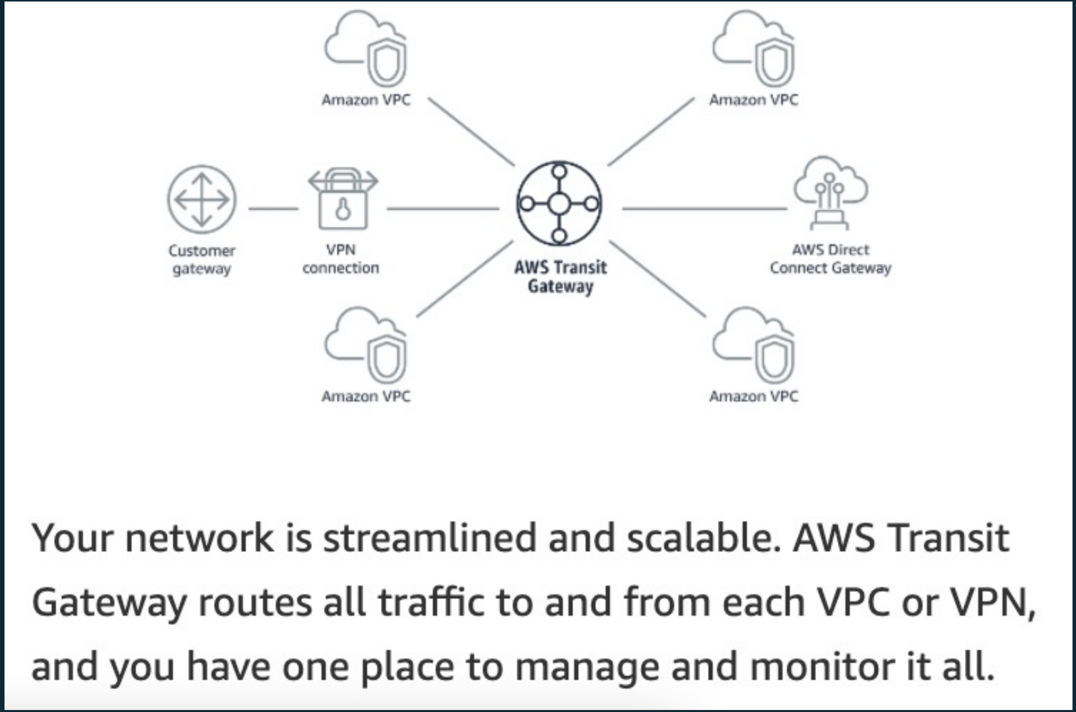
AWS Transit Gateway

Regional Gateway

Simple regional gateway to easily manage VPC connectivity

Massive scale

Attach thousands of VPCs, VPN and Direct Connect connections



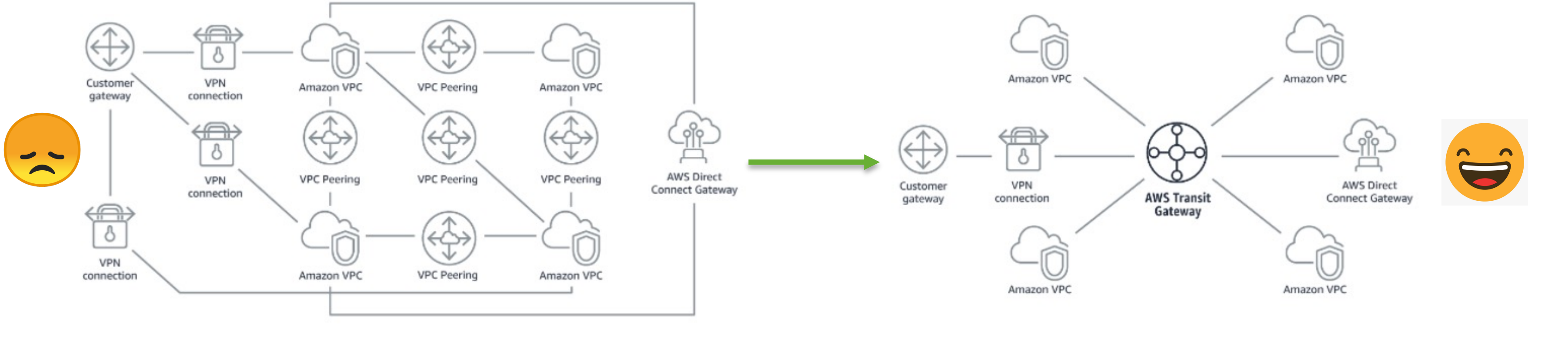
Your network is streamlined and scalable. AWS Transit Gateway routes all traffic to and from each VPC or VPN, and you have one place to manage and monitor it all.

Partner integration

Support for middle-boxing of partner appliances

Without Transit Gateway

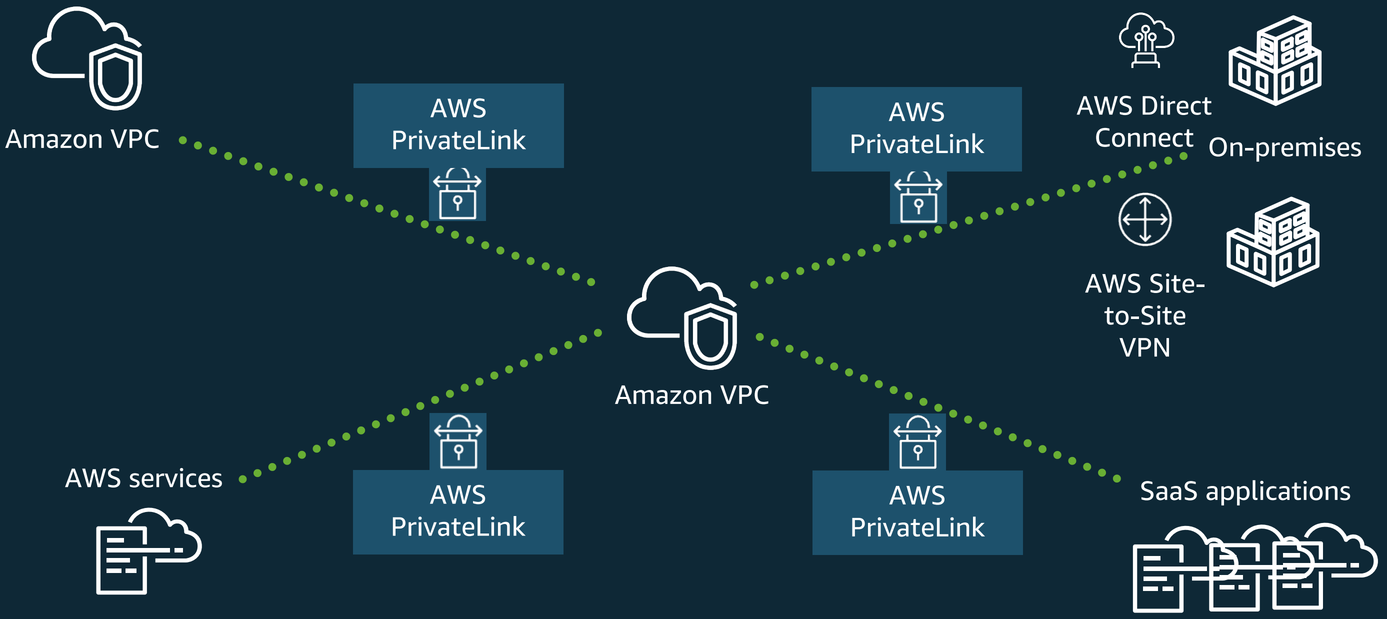
With Transit Gateway



Complexity increases with scale. You must maintain routing tables within each VPC and connect to each onsite location using separate network gateways.

Your network is streamlined and scalable. AWS Transit Gateway routes all traffic to and from each VPC or VPN, and you have one place to manage and monitor it all.

AWS PrivateLink



100+ AWS services

2020 additions:
Lambda, Amazon Redshift, and >35 more

500+ partner integrations

Elastic Load Balancing

Benefits

- Distributed incoming traffic across multiple targets
- TLS offloading and user authentication
- Capable of handling rapid changes in traffic
- Cost effective

Key advancements

Support for redirects and fixed responses

Slow start support for newly registered targets

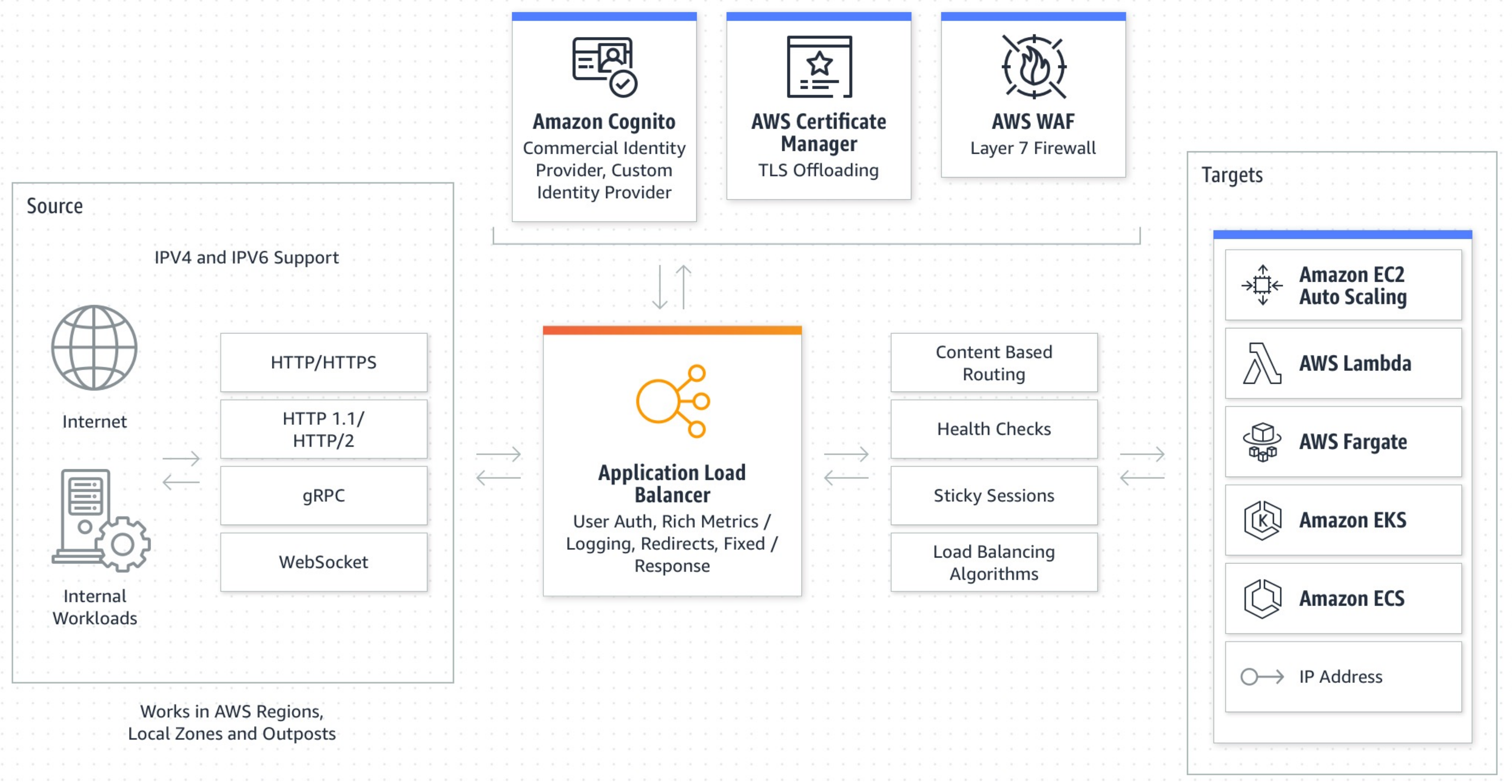
Cross-zone load balancing for Network Load Balancer

Application Load Balancer support for user authentication

Tag-based filtering in API and Management Console

Application Load Balancer | Network Load Balancer | Gateway Load Balancer

Application Load Balancer



Amazon Cognito
Commercial Identity Provider, Custom Identity Provider

AWS Certificate Manager
TLS Offloading

AWS WAF
Layer 7 Firewall

Source

IPV4 and IPV6 Support

Internet

Internal Workloads

HTTP/HTTPS

HTTP 1.1/ HTTP/2

gRPC

WebSocket

Application Load Balancer
User Auth, Rich Metrics / Logging, Redirects, Fixed / Response

Content Based Routing

Health Checks

Sticky Sessions

Load Balancing Algorithms

Targets

Amazon EC2 Auto Scaling

AWS Lambda

AWS Fargate

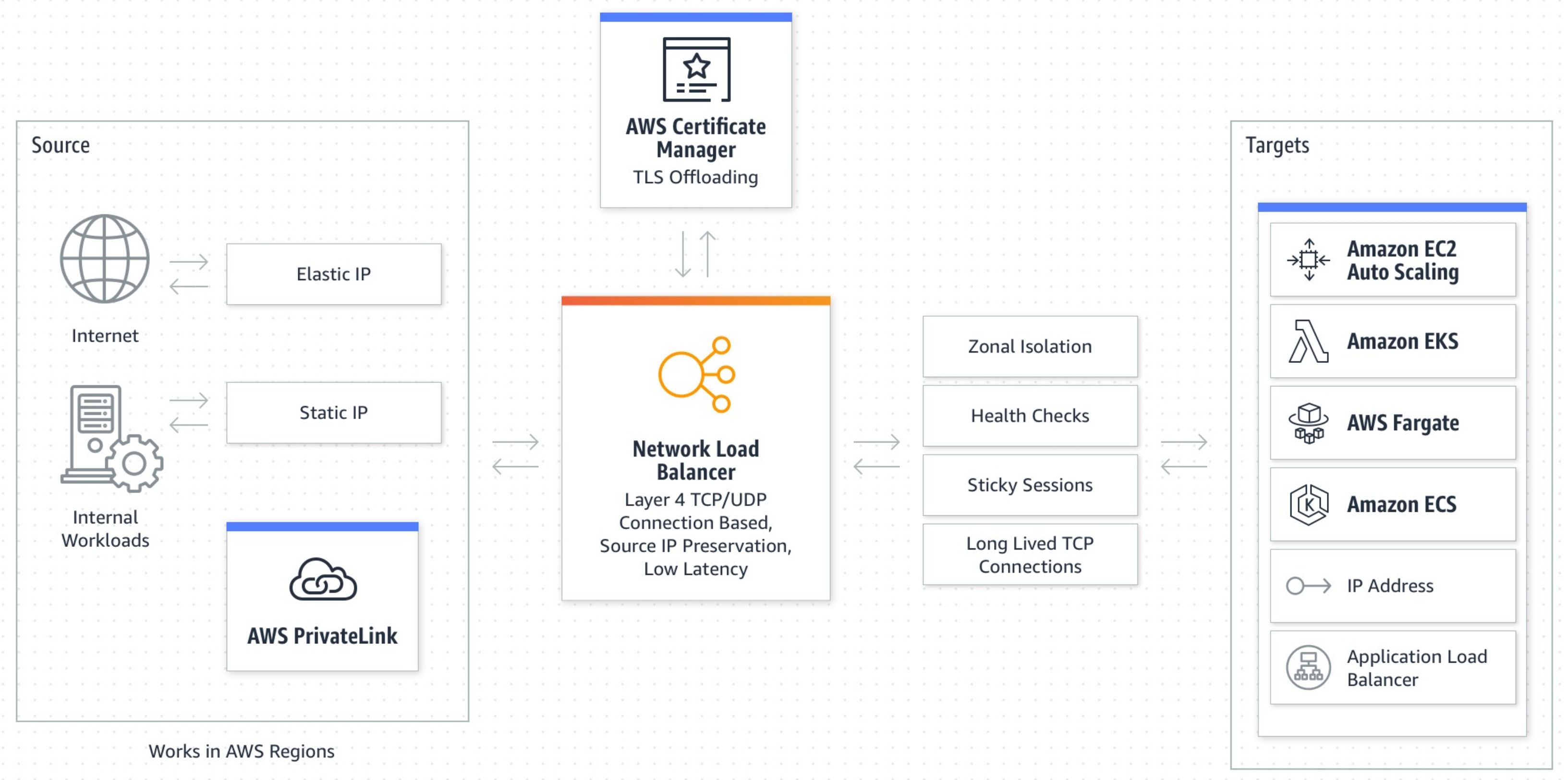
Amazon EKS

Amazon ECS

IP Address

Works in AWS Regions, Local Zones and Outposts

Network Load Balancer



Source

Internet

Elastic IP

Internal Workloads

Static IP

AWS PrivateLink

Works in AWS Regions

AWS Certificate Manager

TLS Offloading

Network Load Balancer

Layer 4 TCP/UDP Connection Based, Source IP Preservation, Low Latency

Zonal Isolation

Health Checks

Sticky Sessions

Long Lived TCP Connections

Targets

Amazon EC2 Auto Scaling

Amazon EKS

AWS Fargate

Amazon ECS

IP Address

Application Load Balancer

AWS Route 53

Benefits

Highly scalable, resilient, managed DNS

Faster traffic routing and lower latency

100% availability SLA

Improved security through granular access controls

Key capabilities

Register and Manage Domains

Manage Hosted Zones

Serve DNS Queries

Traffic Flow routes traffic through end points based on network conditions

Route 53 Resolver provides recursive domain name look-up for VPC and on-premises networks

Amazon CloudFront

Benefits

Fast, massively scaled and globally distributed

Highly programmable

Network and application protection at the edge

Deep Integration with AWS

Key capabilities

>225 Points of Presence Globally

Improved applications security with access control and HTTPs/TLS 1.3 encrypted connections

Better availability with origin fail-over, Lambda@Edge programmable re-directs, and real-time logs

Improved performance with Origin Shield and request compression

Supports dynamic and static content delivery

hulu prime video slack Canon

aws