AWS CLOUD PRACTITIONER

Michael J. Shannon

CISSP, CCSP, CCSK,
SecurityX
ITIL 4 Managing
Professional

Class will begin at 10:00 am
Central Standard Time

AWS CLF-C02

- According to AWS:
  “The Certified Cloud Practitioner validates foundational, high-level understanding of AWS Cloud, services, and terminology.

  This is a good starting point on the AWS Certification journey for individuals with no prior IT or cloud experience switching to a cloud career or for line-of-business employees looking for foundational cloud literacy.”

CLF-C02 Exam Overview

Category	Foundational
Exam duration	90 minutes
Exam format	65 questions; either multiple choice or multiple response
Cost	100 USD (the least expensive AWS exam)
Test in-person or online	Pearson VUE testing center or online proctored exam
Languages offered	English, Japanese, Korean, Simplified Chinese, Traditional Chinese, Bahasa (Indonesian), Spanish (Spain), Spanish (Latin America), French (France), German, Italian, and Portuguese (Brazil)

What is Cloud Computing

- "Cloud computing is the on-demand delivery of compute power, database, storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing"
- "Whether you are running applications that share photos to millions of mobile users or you’re supporting the critical operations of your business, a cloud services platform provides rapid access to flexible and low-cost IT resources"

https://docs.aws.amazon.com/whitepapers/latest/aws-overview/what-is-cloud-computing.html

Trade Fixed Expense for Variable Expense

Only pay for what is needed and used

- Customers can pay only when they consume computing resources
- The default model is to only pay for what is consumed, much like a utility bill
- Reduce upfront capital expenditures by avoiding heavy investments in server farms, data centers, and blade server stacks before you know how you are going to use them

Economies of Scale

- This concept refers to the ability to lower costs and raise efficiency when operating at a larger scale in comparison to operating at a smaller scale
- Since cloud customers are becoming more motivated and willing to drive growth through technology, they often look to strategies such as cost-reducing while enabling innovation

Economies of Scale

Traditional infrastructure

Equipment

Resources and administration

Contracts

Cost

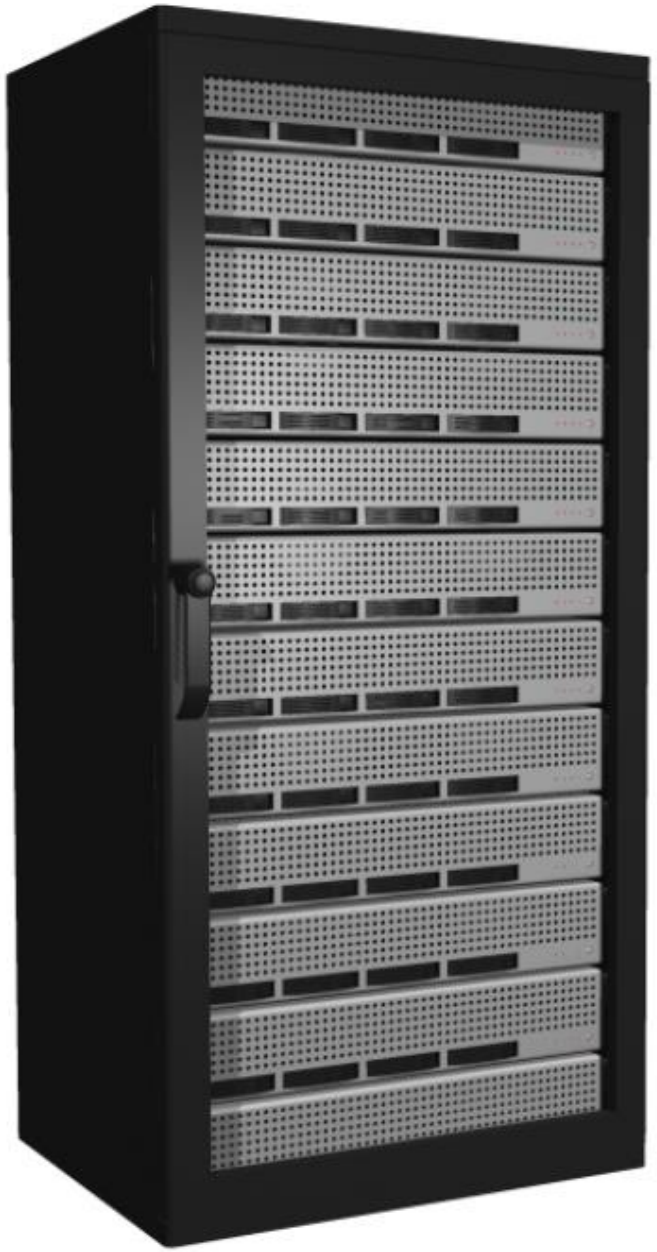
AWS Cloud

No upfront expense, pay for what you use

Improve time to market and agility

Scale up and down

Self-service infrastructure



Stop Guessing Capacity

- Remove the need to guess about infrastructure and service capacity needs
- Customers typically find themselves either sitting on costly idle resources or struggling with inadequate capacity
- Proper capacity decisions can be made prior to application deployment
- A cloud consumer can access as much or as little capacity as needed, and scale up and down as required, with only a few minutes notice

Stop Spending Money Running and Maintaining Data Centers

- Cloud customers can prioritize projects and propositions that set the business apart from competitors rather than the infrastructure
- AWS cloud computing lets organizations focus on their own customers instead of the overhead and heavy lifting of racking, stacking, and powering racks of server blades
- Large and unsustainable data centers will become a thing of the past due to global cloud consuming

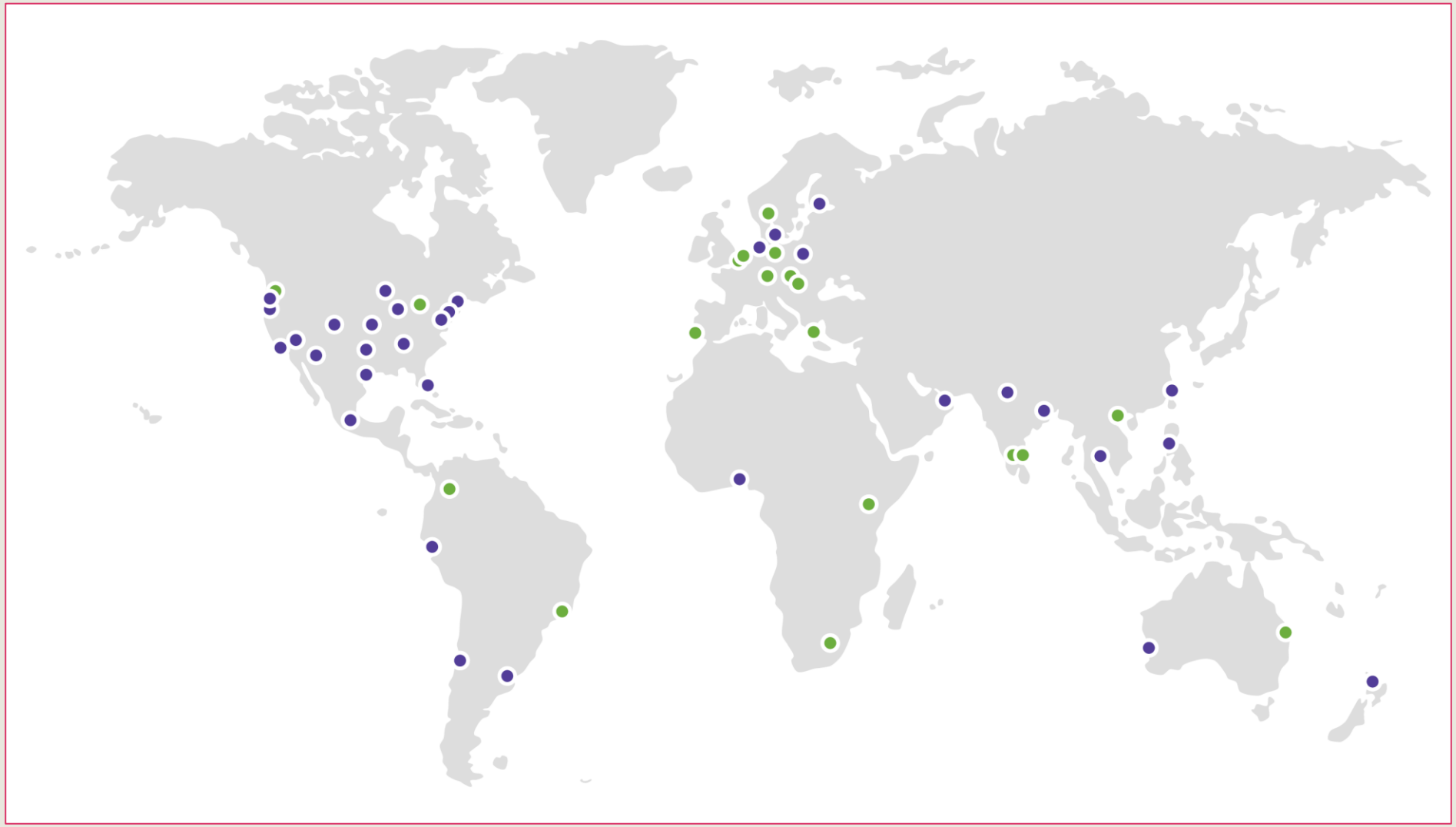
Increase Speed and Agility

- Cutting-edge IT resources are only a click away in a cloud computing environment
- Customers decrease the time to make resources available to administrators and developers from weeks to merely minutes
- The outcome of cloud computing is a substantial increase in agility for the enterprise
  - The resources (cost and time) necessary to experiment and develop are considerably lower

Go Global in Minutes

- Organizations can effortlessly deploy data and applications in several regions around the world with just a few simple clicks
  - This results in lower latency and a better experience for customers at a minimal cost
- AWS customers are leveraging edge locations and availability zone data centers in over 30 geographic regions throughout the world
- New availability zones and regions are added every year

AWS Cloud Infrastructure (Local Zones)



Using Multiple Availability Zones

- Every AWS Region is segmented into distinct Availability Zones (AZs)
- Each AZ has its own power, cooling, and network connectivity forming an isolated failure domain
- Within the AWS domain, customers are encouraged to run their workloads in more than one AZ
- This ensures that customer applications can survive even a complete AZ failure – a very rare event at AWS

Using Multiple Availability Zones

- Objects in a Simple Storage Service (S3) Standard tier are replicated across three availability zones in a region
- In an Amazon Relational Database Service (RDS) Multi-AZ deployment, Amazon RDS automatically creates a primary database (DB) instance and synchronously replicates the data to an instance in a different AZ in the same region
- When a failure occurs and is detected, RDS automatically fails over to a standby instance without manual intervention

Using Multiple Regions

- Customers can deploy applications in multiple AWS regions
- Using multiple regions gives them greater control over their recovery time in the event of a hard dependency failure on a regional AWS service
- Many organizations will use the Route 53 Domain Name System (DNS) service or Global Accelerator IPv6 Anycasting to load balance packets across multiple regions

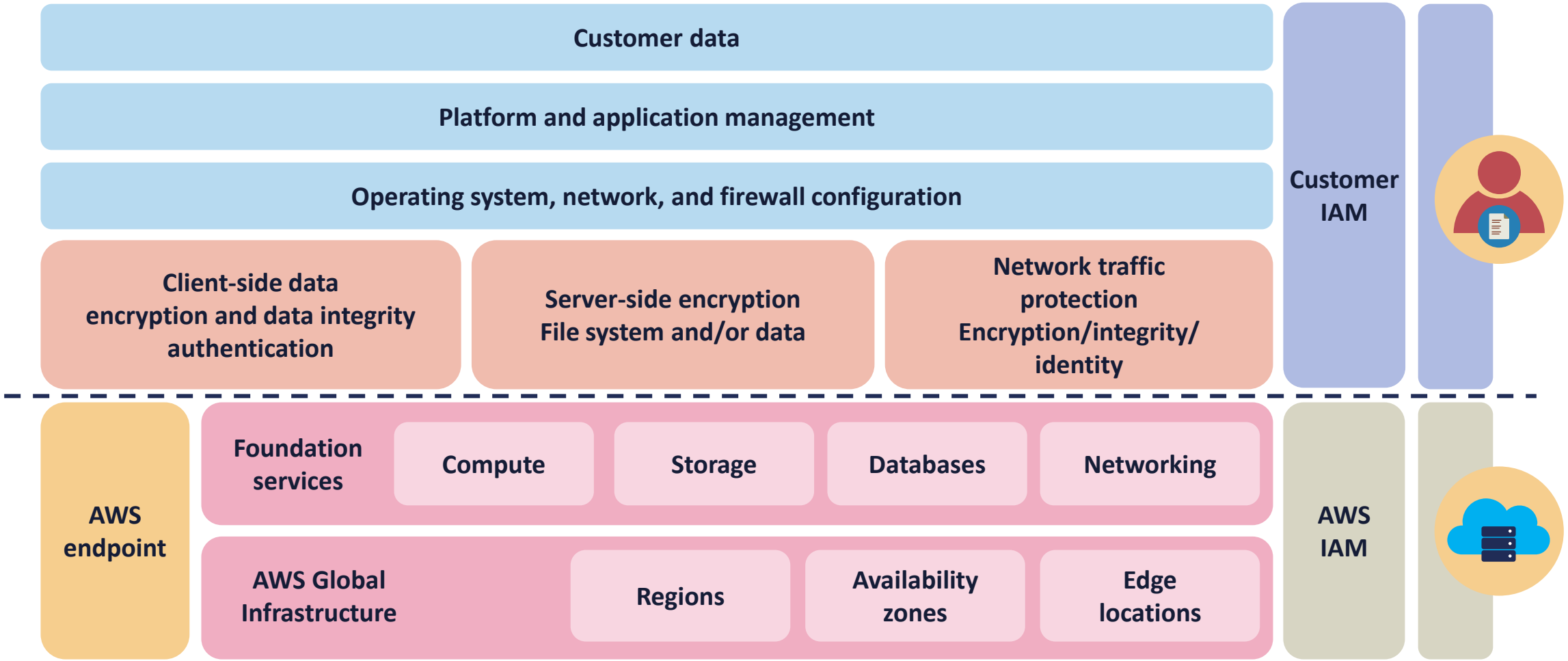
Using Multiple Regions

- Common reasons to utilize multiple AWS regions:
  - Disaster recovery as part of business continuity
  - Lowering latency for customers in different regions
  - Data dispersion initiatives
  - Data sovereignty

Infrastructure-as-a-Service (IaaS)

- Offers the basic building blocks for cloud information technology
- Provides access to networking features, computers (virtual or on dedicated hardware), and data storage space in the AWS data center
- Delivers customers the highest level of flexibility and management control over their IT resources
- Compares to existing IT resources that many IT departments and developers are familiar with today

AWS Infrastructure-as-a-Service (IaaS)



Platform-as-a-Service (PaaS)

- Removes the need for organizations to manage the underlying infrastructure (usually hardware and operating systems)
- Allows customers to focus on the deployment and management of their applications
- Allows customers to relax and not be concerned with resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running applications or databases

AWS Platform-as-a-Service (PaaS)

Development and software development kit (SDK) platforms for Java, PHP, Python, etc.

Container services for Docker and Kubernetes

Managed and fully managed relational and document databases

Managed security and threat modeling services

Single sign-on (SSO), machine learning, artificial intelligence (AI), Internet of things (IoT), blockchain, media services

Software-as-a-Service (SaaS)

- SaaS offers customers a comprehensive solution run and managed by the service provider
- In most cases, this involves various end-user applications
- With a SaaS offering, customers are not involved with the maintenance of the service or underlying infrastructure
- A common example of a SaaS application is web-based email or personal cloud storage

Common SaaS Offerings

- Customer relationship management (CRM)
- Enterprise resource management (ERM)
- Human resources and workplace tools
- Finance, sales, and marketing services
- Payroll services
- Email, collaboration, and cloud storage
- Help desk and service desk
- Virtual call center
- Business analytics

Cloud Deployment Models: Cloud

- A cloud-based application is fully deployed in the cloud, and all parts of the application or database solution run in the cloud
- Applications in the cloud have either been generated in the cloud or have been migrated from a standing infrastructure to leverage the benefits of AWS cloud computing
- Cloud-based applications can be constructed on low-level infrastructure pieces or can use higher-level services that offer abstraction from the management, architecting, and scaling needs of the core infrastructure

Cloud Computing Deployment Models: Hybrid

- This model is a method for connecting infrastructure and applications between cloud-based resources and existing resources that are not placed in the cloud
- The most common method is between the cloud and existing on-premises infrastructure to extend and grow an organization's infrastructure into the cloud while connecting cloud resources to internal systems
- Online retailers may use hybrid cloud for "bursting up"

Cloud Deployment Models: On-Premises

- Installing resources on-premises, using virtualization and resource management tools, often called private cloud
- On-premises deployment does not provide many of the benefits of cloud computing but is often chosen for its ability to provide dedicated resources
- In most scenarios, this deployment model is the same as legacy IT infrastructure while using application management and virtualization technologies to try and increase resource utilization

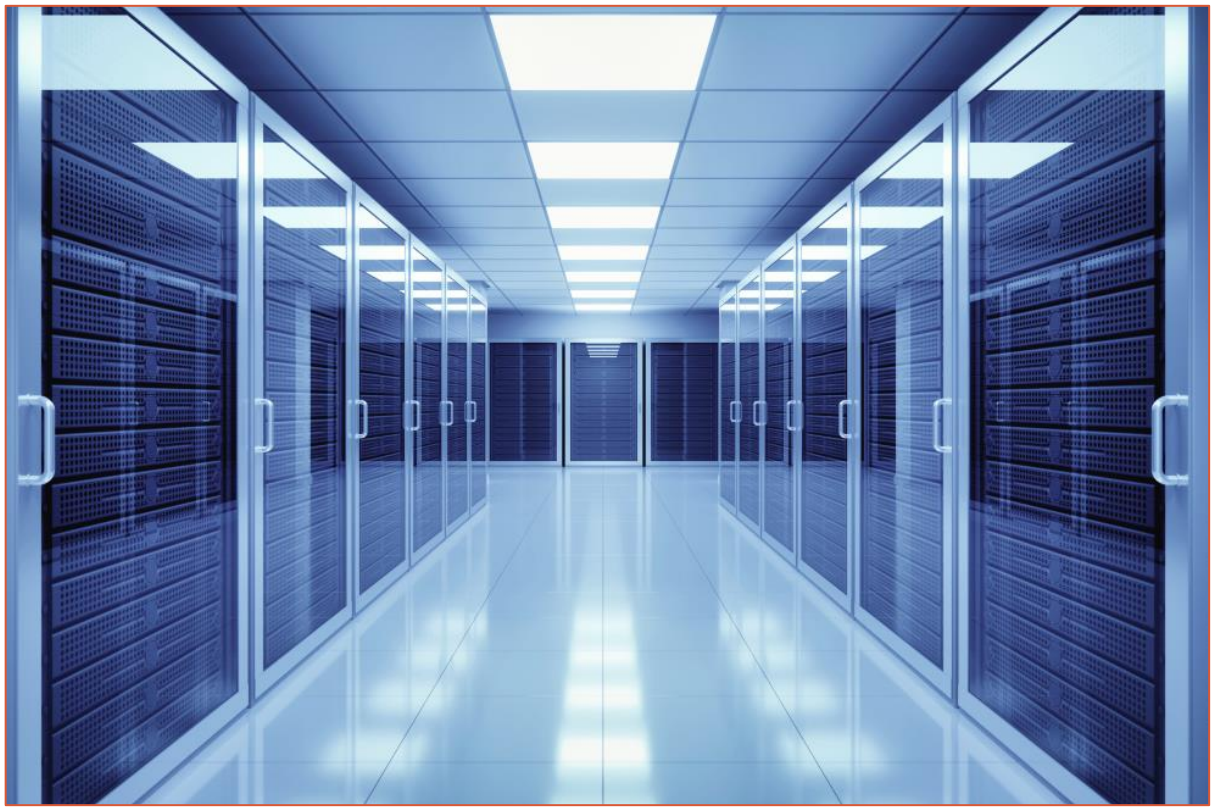
AWS Shared Responsibility Model

- Security and compliance are shared responsibilities between AWS and the cloud customer
- AWS operates, manages, and optimizes the components from the host operating system and virtualization layer all the way down to the physical security of the Availability Zone data centers in which the services operate

AWS Shared Responsibility Model

- Customers should carefully evaluate the selected services
- Their responsibilities vary, contingent on the services used, the integration of those services into their IT environment, and any relevant laws and regulations
  - **This is highly applicable to the Platform as a Service (PaaS) models**
- The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment

AWS Responsibilities



- AWS is responsible for defending the infrastructure that runs all the services offered in the AWS Cloud
- This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services all over the world
- The customer fully inherits the physical and environmental controls from AWS

Shared Responsibility

- AWS responsibility: security **of** the cloud
- Customer responsibility: security **in** the cloud

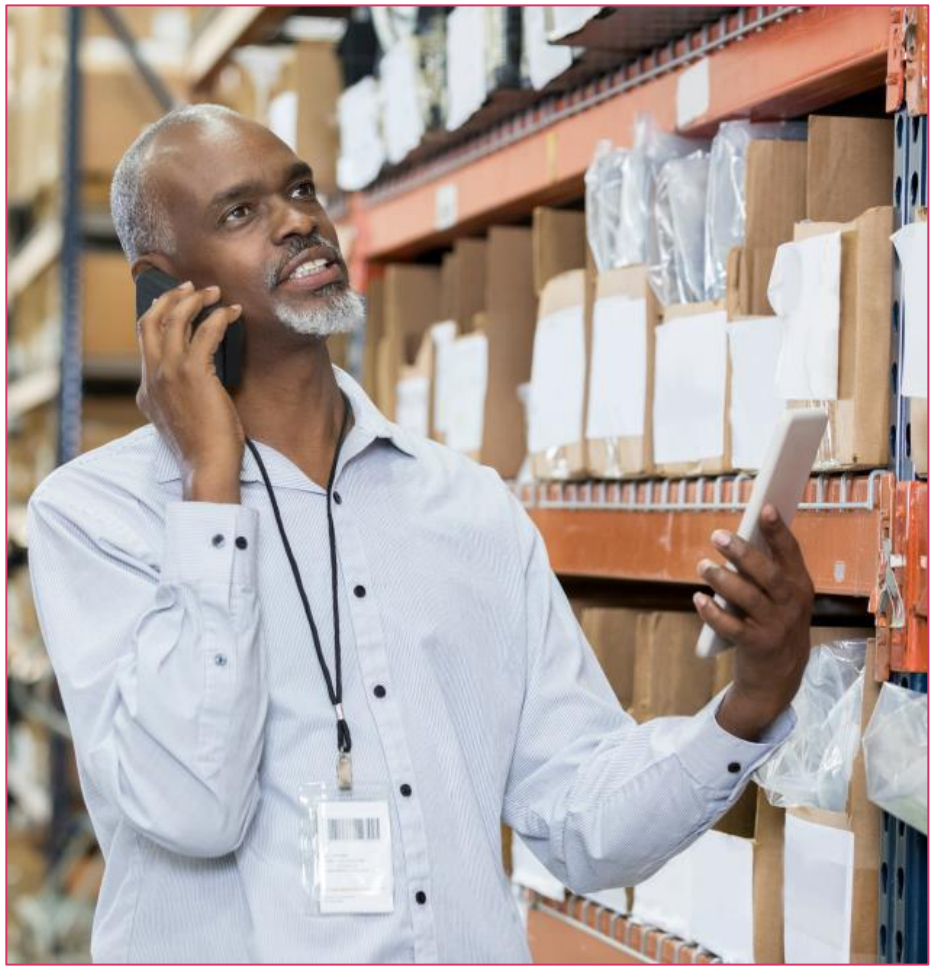
Shared Controls

- **Patch management** – AWS must patch and fix configuration flaws within the infrastructure, but customers are responsible for patching their guest operating systems and applications
- **Configuration management** – AWS preserves the configuration of its infrastructure devices, but customers are responsible for configuring their own guest operating systems, databases, and applications
- **Awareness and training** - AWS trains AWS employees, but the customer must provide their own training for their own employees

Customer Responsibilities on AWS

- Customer responsibility will be driven by the cloud services that a customer chooses
- This will dictate the amount of configuration tasks the customer will conduct as part of their security responsibilities
- For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is considered an IaaS type, therefore it demands the customer perform all the necessary security configuration and management duties

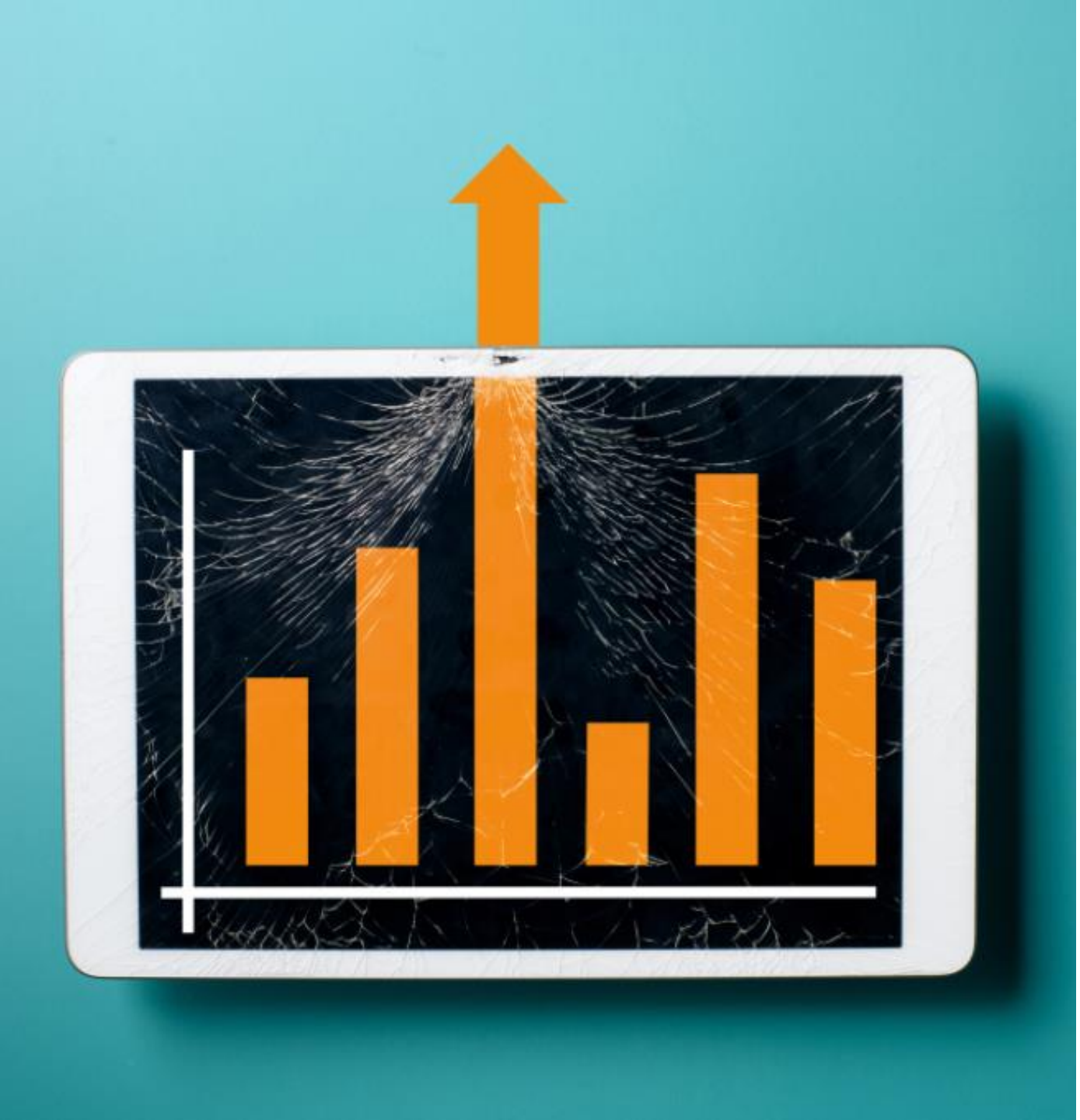
Customer Responsibilities on AWS



- Customers that deploy an EC2 instance are responsible for managing:
  - The guest operating system (including updates and security patches)
  - Any application software or utilities installed by the customer on the instances
  - Configuration of the AWS-provided firewall (called a security group) on each instance

Advantages of High Availability

- Protect against data center, availability zone (AZ), server, network, and storage subsystem failures:
  - Keep your organization or business running with little or no downtime
- All AZs in an AWS region are interconnected with high-bandwidth, low-latency networking, over fully redundant, dedicated metro fiber
- Data centers located in different AWS AZs have a discrete, uninterruptible power supply and onsite backup generation facilities



Advantages of Elasticity

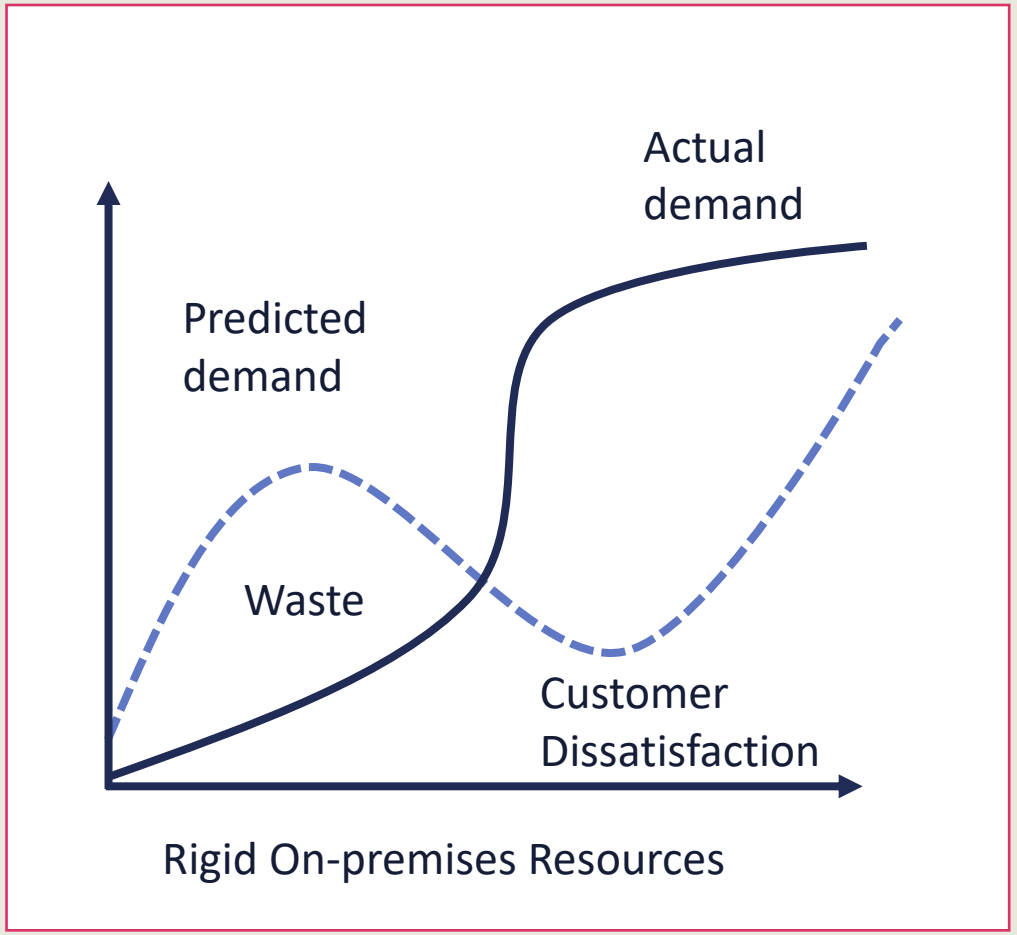
- Elasticity provides the ability to almost instantly provision and de-provision assorted cloud resources:
  - Virtual instances, containers, appliances, database tables, and more
- It involves leveraging dynamic auto-scaling technologies
- Challenges with predicting demand leads to higher costs for the enterprise
- Recent circumstances have revealed how de-provisioning may be the more vital aspect of elasticity

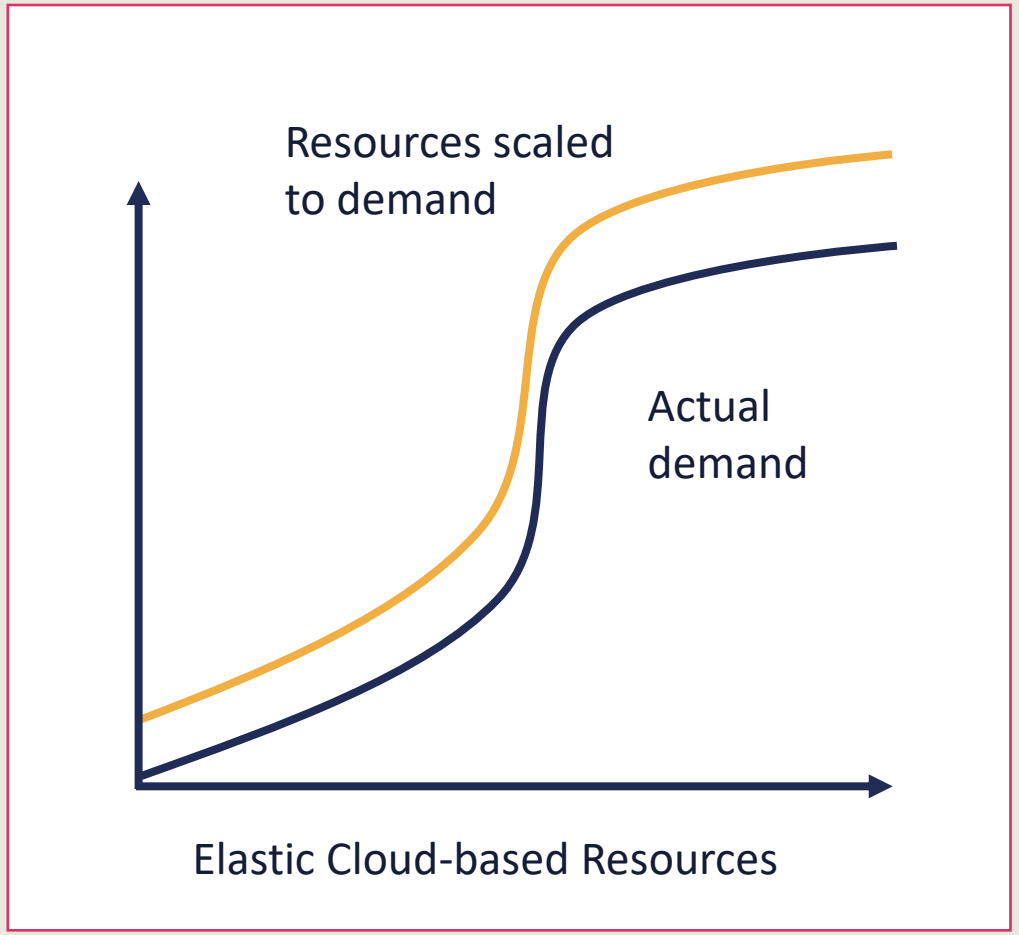
Advantages OF Elasticity

"Elasticity of the cloud allows us to add thousands of virtual servers and petabytes of storage within minutes, making such an expansion possible...Leveraging multiple AWS cloud regions, spread all over the world, enables us to dynamically shift around and expand our global infrastructure capacity, creating a better and more enjoyable streaming experience for Netflix members wherever they are"

– Yury Izrailevsky, VP Cloud and Platform Engineering, Netflix (from Netflix Media Center)

Elasticity


Actual
demand
Predicted
demand
Waste
Customer
Dissatisfaction
Rigid On-premises Resources


Resources scaled
to demand
Actual
demand
Elastic Cloud-based Resources

Advantages of Agility

- Agility leverages features for rapid deployment, testing, experimentation, and innovation
- Customers can quickly overcome geographical limitations
- Content creators can get customer content as close to the consumer as possible
- Agility means reducing time and costs for testing, innovation, and experimentation

Cloud Adoption Strategies: Rehosting

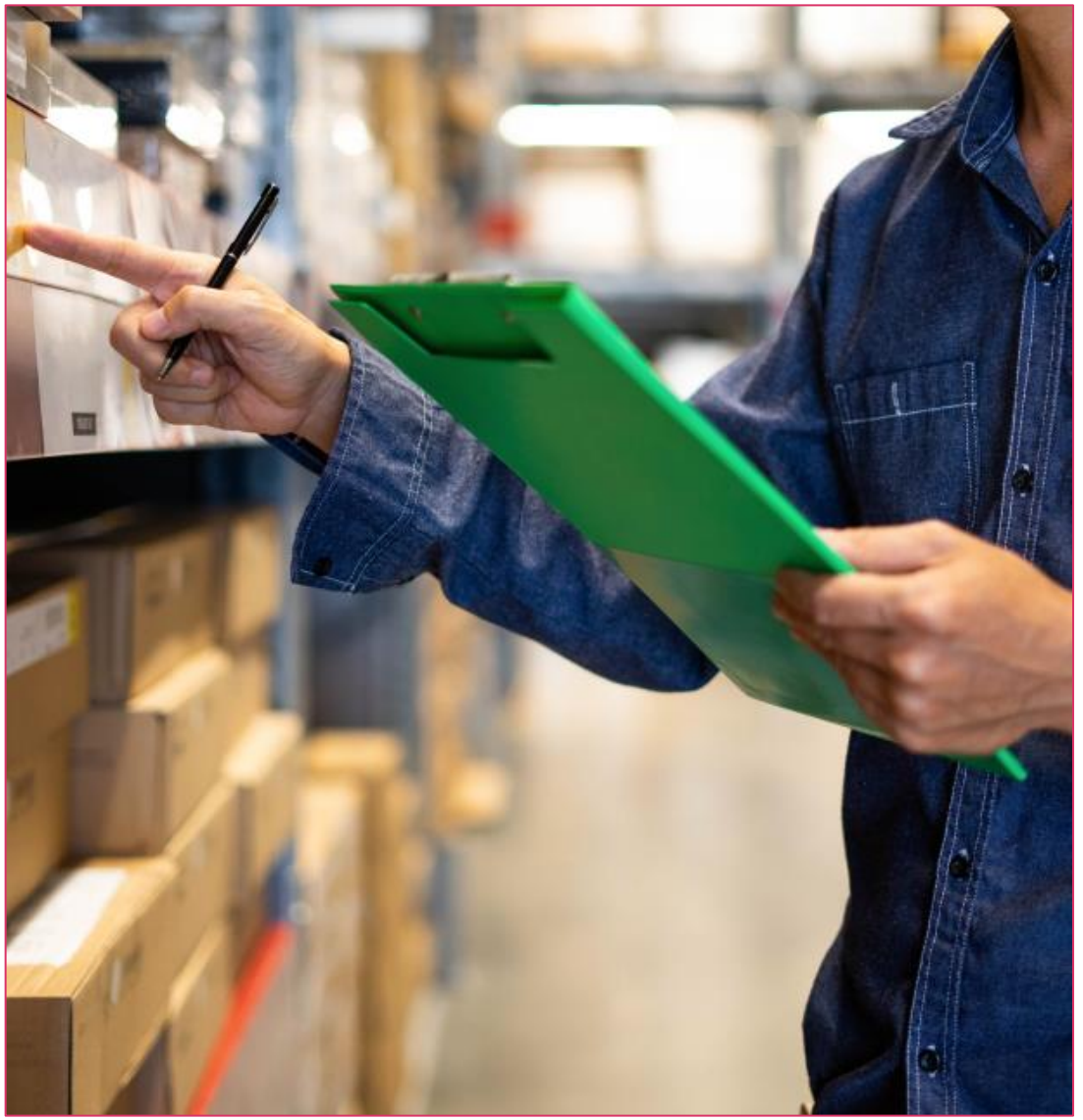
- This is also known as "lift-and-shift"
- Most applications are rehosted since the organization is looking to scale its migration quickly to meet a certain business case
- Most rehosting can be automated with tools provided by AWS:
  - Some customers still prefer to do this manually as they learn how to apply their legacy systems to the new cloud platform
- Many applications are easier to optimize and rearchitect once they are already running in the cloud

Cloud Adoption Strategies: Replatforming

- This is sometimes called "lift-tinker-and-shift"
- The customer might make a few cloud (or other) optimizations in order to achieve some tangible benefits
- Otherwise, they are not changing the core architecture of the application:
  - Examples to be explored later will be migrating to an Amazon Relational Database Service (RDS)

Cloud Adoption Strategies: Repurchasing

- This strategy involves moving to a different product or vendor solution
- A common example is moving to a SaaS solution for enterprise resource planning (ERP) or customer relationship management (CRM)



Cloud Adoption Strategies: Refactoring or Rearchitecting

- This would involve reimagining how the application is architected and developed, often using cloud-native solutions
- Common use case is when a business must add features, scalability, or performance that would otherwise be challenging to achieve in the application's current environment
- A more expensive option for organizations looking to migrate from a monolithic architecture to a service-oriented environment

Cloud Adoption Strategies: Retiring

- An application or service has reached the disposition phase because of
  - Supply chain challenges
  - End of life or end of support
  - Deprecated technology
  - Regulations or compliance
  - No more utility

Cloud Adoption Strategies: Retaining

- This typically means to "revisit" or do nothing for the foreseeable future
- The company may still be "riding out" some depreciation
- There is not a present inclination to migrate some applications until there are changes to the business cycle, socio-political factors, or budgets
- The organization should only migrate what makes sense for the delivery of the value proposition

Cloud Adoption Resources

- **AWS Professional Services** - A global team of experts that can help customers realize their desired business outcomes
- **AWS Solutions Architects** - Certified cloud architects
- **AWS Activate for Startups** - Free templates, tools, resources, content, and expert support to accelerate the startup
- **AWS Knowledge Center** - helps answer the questions most frequently asked by AWS Support customers
- **AWS Compliance**
- **The AWS Cloud Adoption Framework**

The AWS Cloud Adoption Framework (CAF)

- The AWS CAF organizes guidance into six areas of focus, called perspectives
- Each perspective speaks to discrete responsibilities
- The planning process assists the right stakeholders across the organization in preparing for the coming changes
- In general, the Business, People, and Governance perspectives focus on business capabilities
- The Platform, Security, and Operations perspectives focus on technical capabilities

- **Envision** - Identify and prioritize transformation opportunities in line with your strategic objectives
- **Align** - Identify capability gaps and cross-organizational dependencies
- **Launch** - Deliver pilots in production and demonstrate incremental business value
- **Scale** - Expand pilots and business value to desired scale

The AWS CAF Governance Perspectives

- **Governance and Compliance** – Establishing policies and standards to ensure cloud adoption aligns with legal, regulatory, and organizational requirements
- **Financial Management** – Managing cloud costs effectively through budgeting, tracking spending, and optimizing resources
- **Risk Management** – Identifying, assessing, and mitigating risks associated with cloud adoption, including security and operational risks
- **Stakeholder Engagement** – Ensuring clear roles and responsibilities among stakeholders to support governance and decision-making
- **Performance Management** – Monitoring key performance indicators (KPIs) to track cloud adoption success and continuous improvement

Costs of On-Premises Environments

- On-premises costs can quickly be burdensome and prohibitive, especially in challenging economic environments:
  - These costs can range from upfront capital to regular operational expenditures that keep the data center running
- Customers are discovering the massive savings in labor costs and other overhead by moving to the AWS cloud
- Although capital expenditures like hardware, racks, and network equipment are a one-time purchase, they typically have a refresh cycle of five years

Cost Savings of Moving to the Cloud

- The value of cloud extends beyond total cost of ownership (TCO) reduction
- AWS customers also see substantial enhancements in other areas, including personnel productivity, operational resilience, and corporate agility
- AWS customers get an average cost savings of 31 percent by migrating to the cloud

Fixed Costs vs. Variable Costs

- The cloud allows customers to trade fixed expenses for variable expenses and only pay for IT as they consume it
- Due to the economies of scale, the variable expenses are much lower than what organizations would pay to do it themselves
- Whether it is a startup in the cloud, or just starting the migration journey to the cloud, AWS has a set of solutions to help manage and optimize expenditures

Fixed Cost Examples

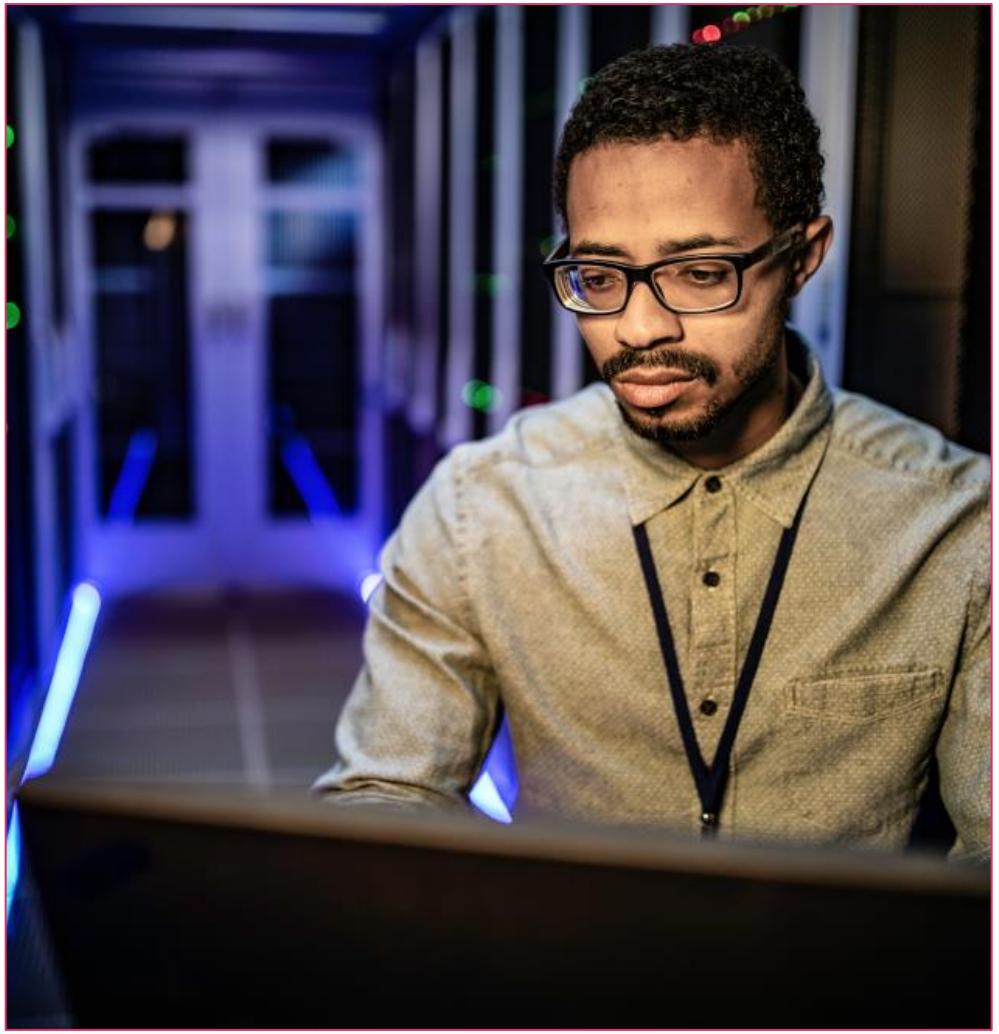
- Data centers and server farms
- Physical blade servers and racks
- Storage area networks (SAN)
- Buildings, HVAC, and environmental controls

Variable Cost Examples

- Virtual instances of Windows and Linux
- Serverless solutions like Functions as a Service (FaaS)
- Relational database services
- Elastic file services

Examining AWS Licensing Strategies

- **Buy licenses from AWS** - using license included instances allows you access to fully compliant Microsoft software licenses bundled with Amazon EC2 or Amazon RDS instances and pay for them as you go with no upfront costs or long-term investments
- **Bring licenses to AWS** - If you've already purchased Microsoft software, you have the option to bring your own licenses (BYOL) to the AWS Cloud (subject to Microsoft license terms):
  - Without software assurance
  - With software assurance

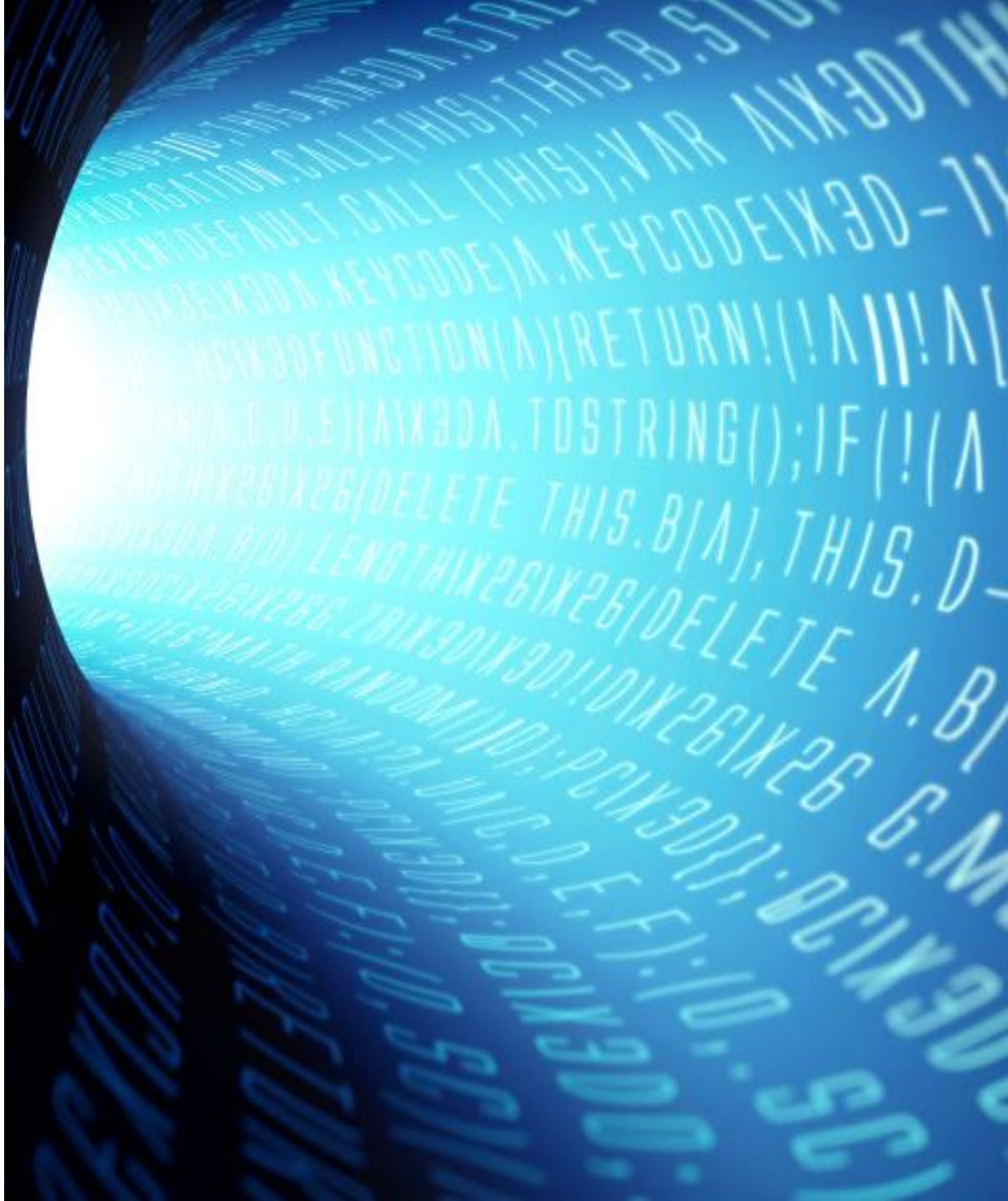


The Right Sizing Concept

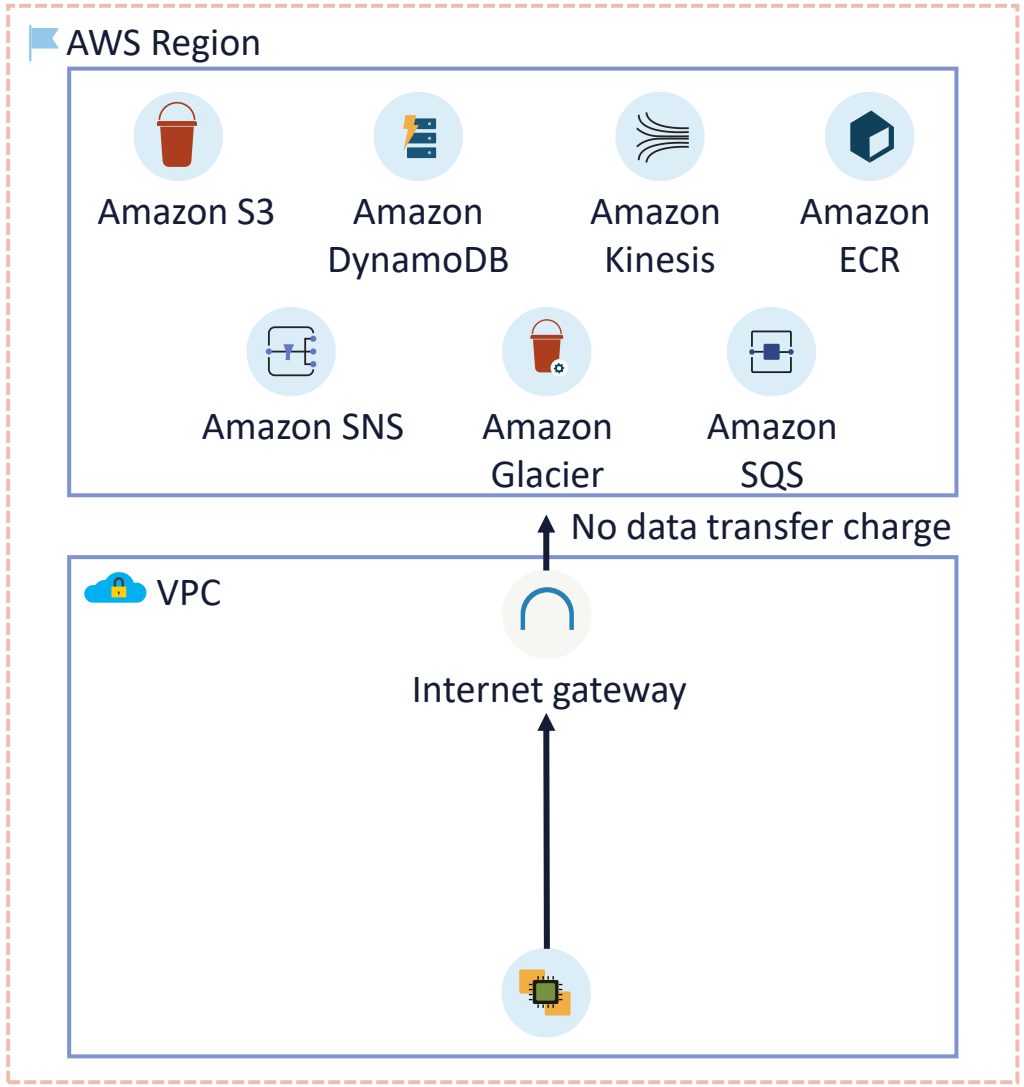
- Right sizing is the practice of mapping instance types and sizes to workload performance and capacity requirements at the lowest feasible cost
- It involves observing deployed instances and recognizing openings to eradicate or downsize without compromising capacity or other requirements
- It is a key mechanism for optimizing costs and is often overlooked by organizations when they first transfer to the AWS Cloud

Data Transfer Charges

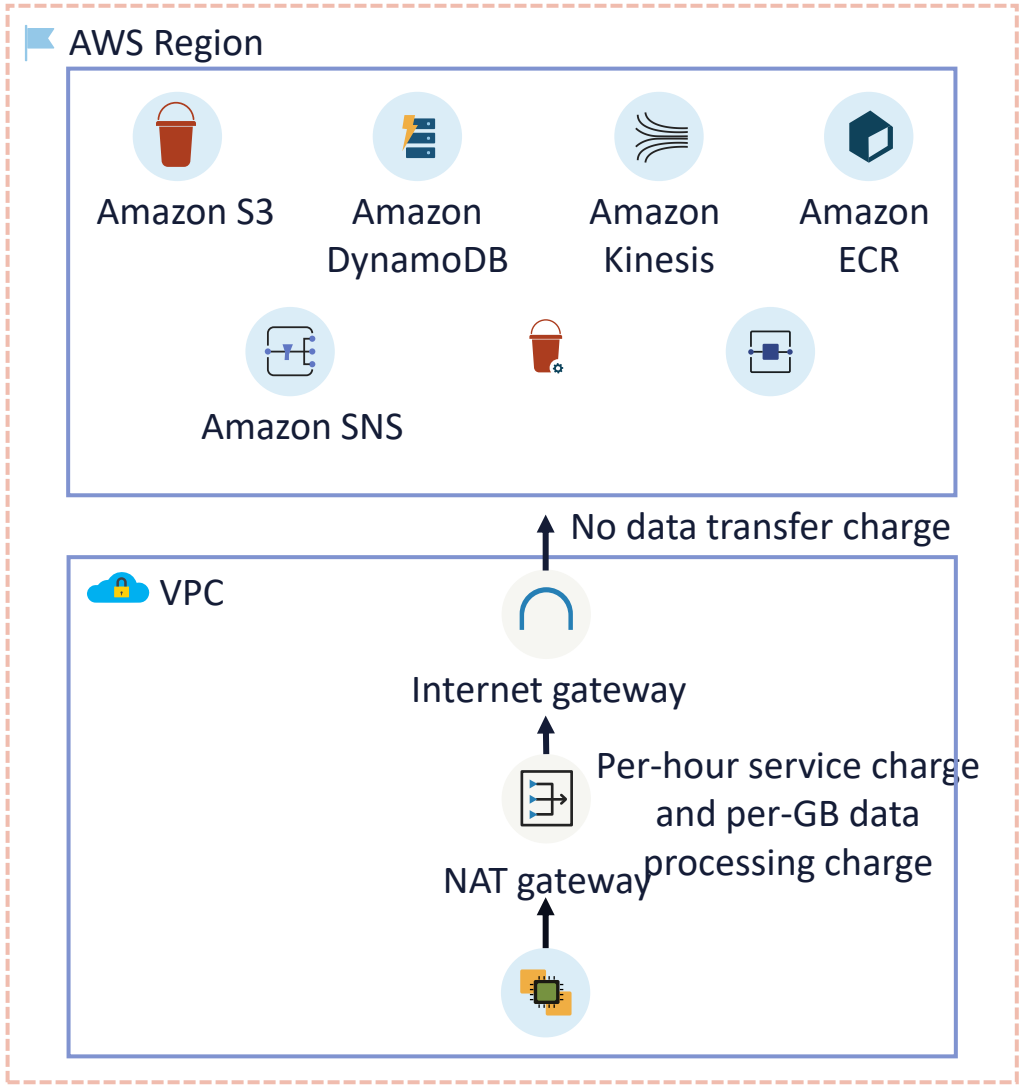
- There is no charge for inbound data transfer across all services in all regions at AWS
- Data transfer from AWS to the Internet is charged per service, with rates specific to the initiating region
- Data transfer within AWS can be from the customer's workload to other AWS services, or it could be between different components of the customer workload
- When a customer workload accesses AWS services, they may invite data transfer charges



Data Transfer Charges

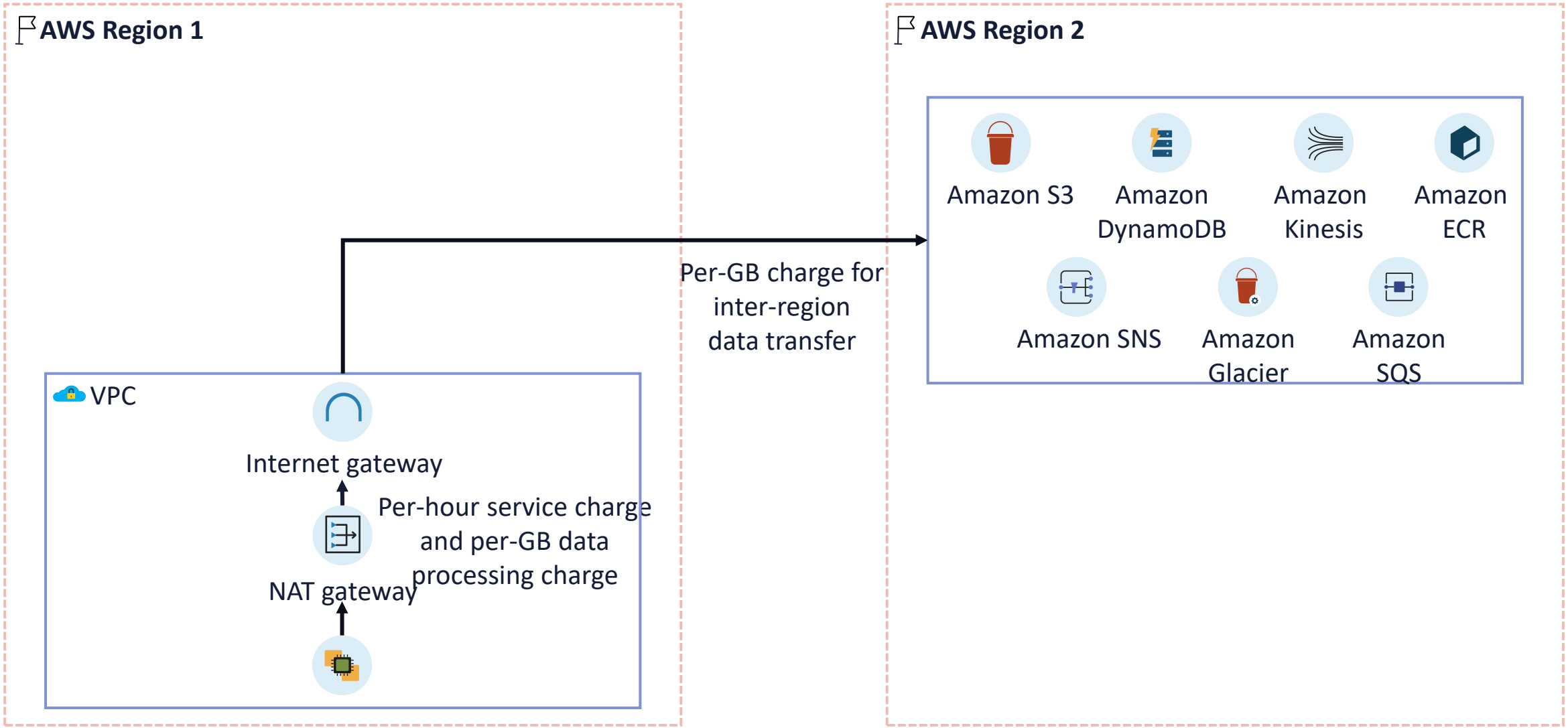


Internet gateway



NAT gateway

Data Transfer Charges



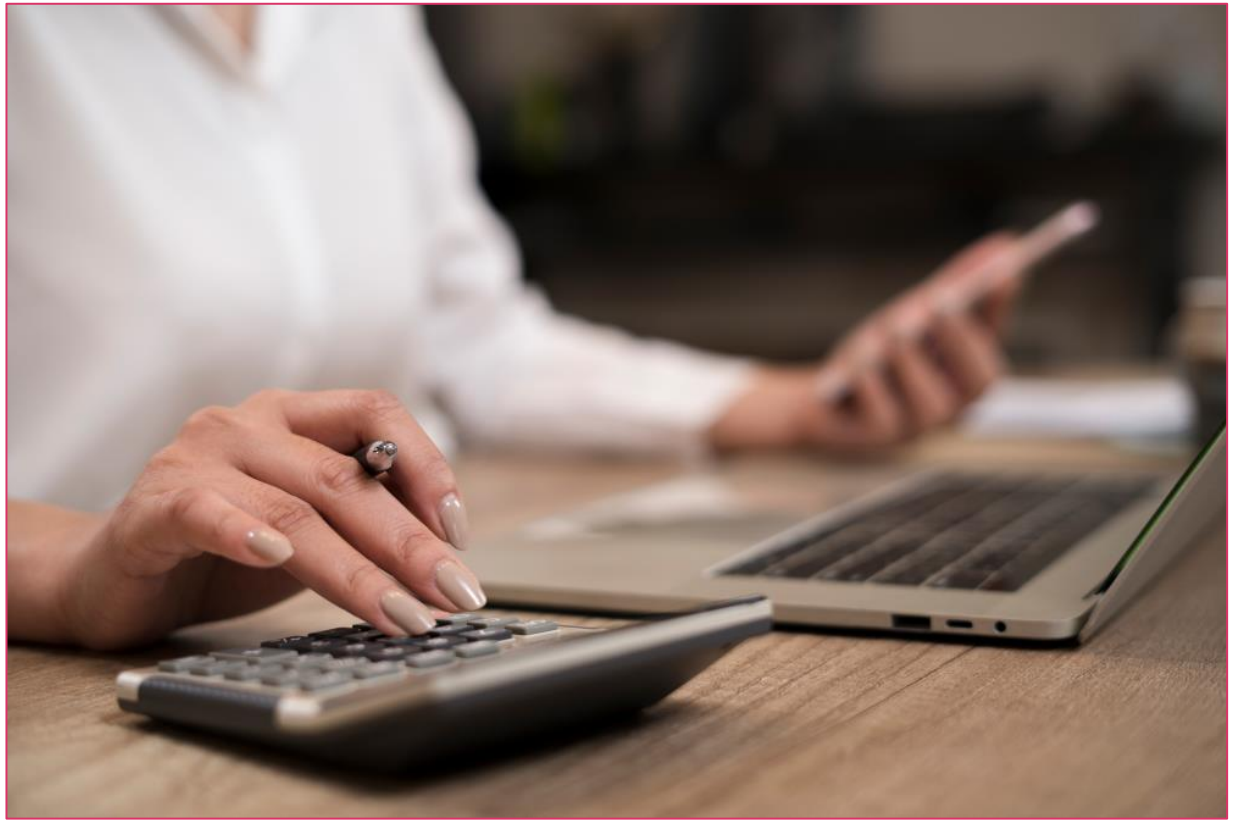
AWS Tags

- A tag is a label that a customer or AWS assigns to an AWS resource
- Every tag is made up of a key and a value
- For each resource, the tag key must be unique, and each tag key can have only a single value
- Customers can use tags to organize their resources

Cost Allocation Tags

- Two types of cost allocation tags:
  - AWS-generated tags
  - User-defined tags
- AWS (or AWS Marketplace ISV) defines, creates, and applies the AWS-generated tags for the customer
- The customer defines, creates, and applies the user-defined tags
- Customers must activate both types of tags separately before they can appear in Cost Explorer or on a cost allocation report

Cost Allocation Tags



- After the tag is applied to AWS resources and the customer activates the tags in the Billing and Cost Management console, AWS then generates a cost allocation report as a comma-separated value (CSV) file with the usage and costs grouped by the active tags
- Applied tags can represent business categories like cost centers, application names, or owners to organize costs across multiple services

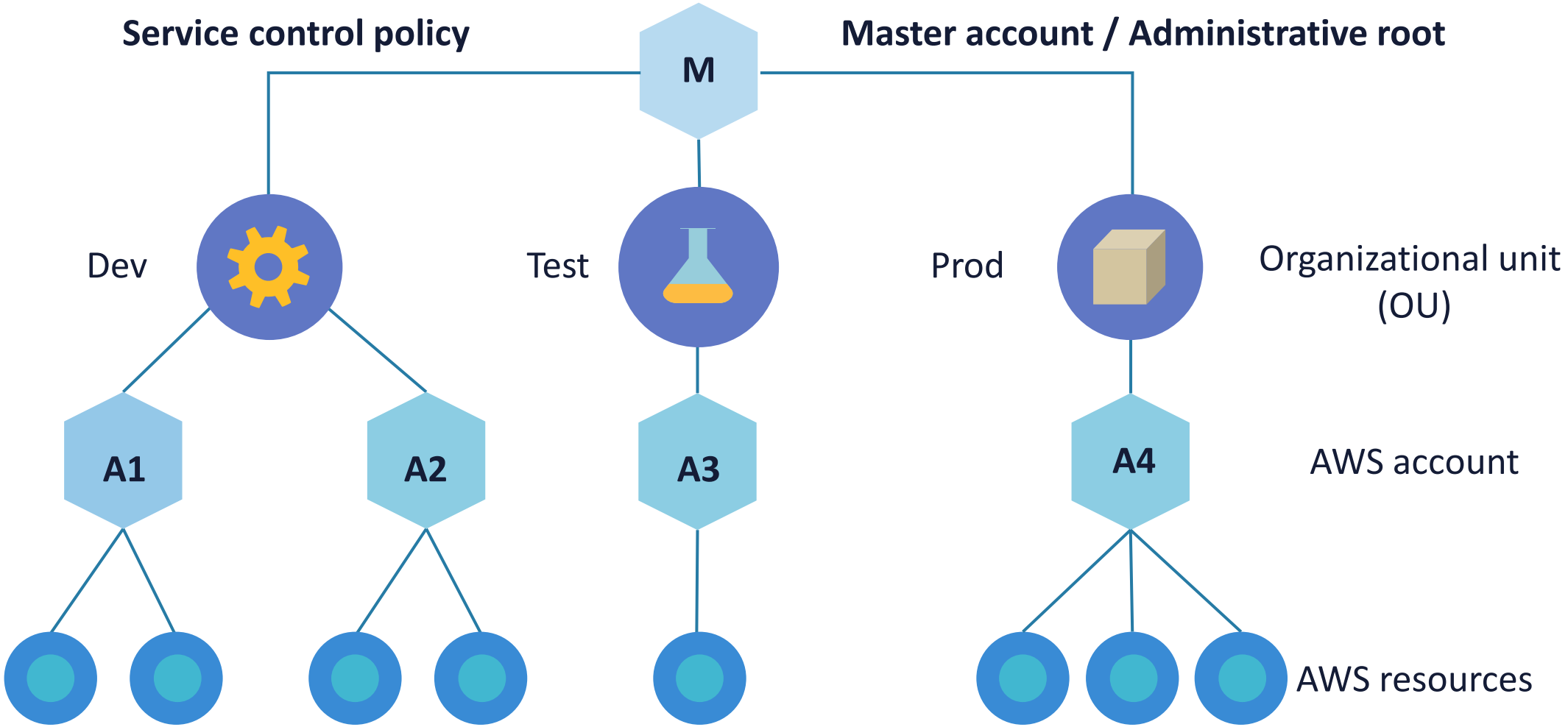
Cost Allocation Tags

Total Cost	User: Owner	User: Stack	User: Cost Center	User: Application
0.89	DbAdmin	Test	80512	Token2
0.03	DbAdmin	Test	80512	Token2
2.99	DbAdmin	Prod	80512	Token2
5.88	DbAdmin	Test	67815	Token1
229.32	SysOpsEng	Prod	67815	Token1
0.73	DbAdmin	Test	67815	Token1
0.02	DbAdmin	Prod	80512	GUI
2.51	DbAdmin	Prod	67815	GUI

AWS Organizations

- AWS Organizations provide policy-based management for multiple AWS accounts, including
  - Creating groups of accounts
  - Automating account creation using console and application programming interfaces (APIs)
  - Applying and managing policies for account groups
- Customers can centrally manage Service Control Policies (SCPs) across multiple accounts without using manual processes:
  - An SCP allows administrators to place guardrails on highly privileged principals with "deny" statements in JSON-managed security policies

AWS Organizations



Comparing AWS Supports Plans

In this demo…

Compare AWS Support plans

AWS Professional Services

- AWS Professional Services is available in the AWS Marketplace
- It allows customers to find and buy assessments, implementation, support, managed services, and training for third-party software and building on AWS
- AWS Marketplace assists customers in finding the software and associated services necessary to transform and simplify cloud service acquisition in one location
- Professional Services offers wide-ranging business solutions and curated service offerings from independent software vendors and consulting partners

AWS Professional Services

Assessment and implementation

Evaluate the current operating environment, explore services, and get help with configuration, setup, and deployment of third-party or AWS native services

Premium support

Get access to direction and aid from independent software vendors and consulting partners targeted to specific needs

Managed services

Achieve end-to-end environment management from independent software vendors or consulting partners that represent the organization

Training

Take advantage of customized workshops, programs, and instructive tools delivered by AWS experts to assist employees in learning best practices

Solutions Architects

- The Solutions Architect team at AWS is tasked with assisting customers in the effective deployment of cloud technologies
- AWS customers can partner with internal AWS teams and leverage a profound knowledge of available tools and products
- They can formulate scalable, agile, and robust cloud architectures that address customer business problems
- As a team member, customers can experiment daily and help drive the future of cloud computing

AWS Solutions Architect Enablement

- An "experiment and fail" culture
- Robust training programs
- Diverse array of certification paths
- Leadership and mentorship programs
- Flexible work-life balance

AWS Partner Network

- The AWS Partner Network (APN) is a global consortium of associates that combines programs, knowledge, and resources to build, market, and sell customer offerings
- It is a diverse network of over 100,000 partners from more than 150 countries
- AWS and partners work to:
  - Deliver inventive solutions
  - Resolve technical issues
  - Win deals and agreements
  - Provide value to mutual customers

AWS Partner Network

Innovate

Take advantage of the newest AWS technologies to test, build, and deliver differentiated customer solutions

Reach customers

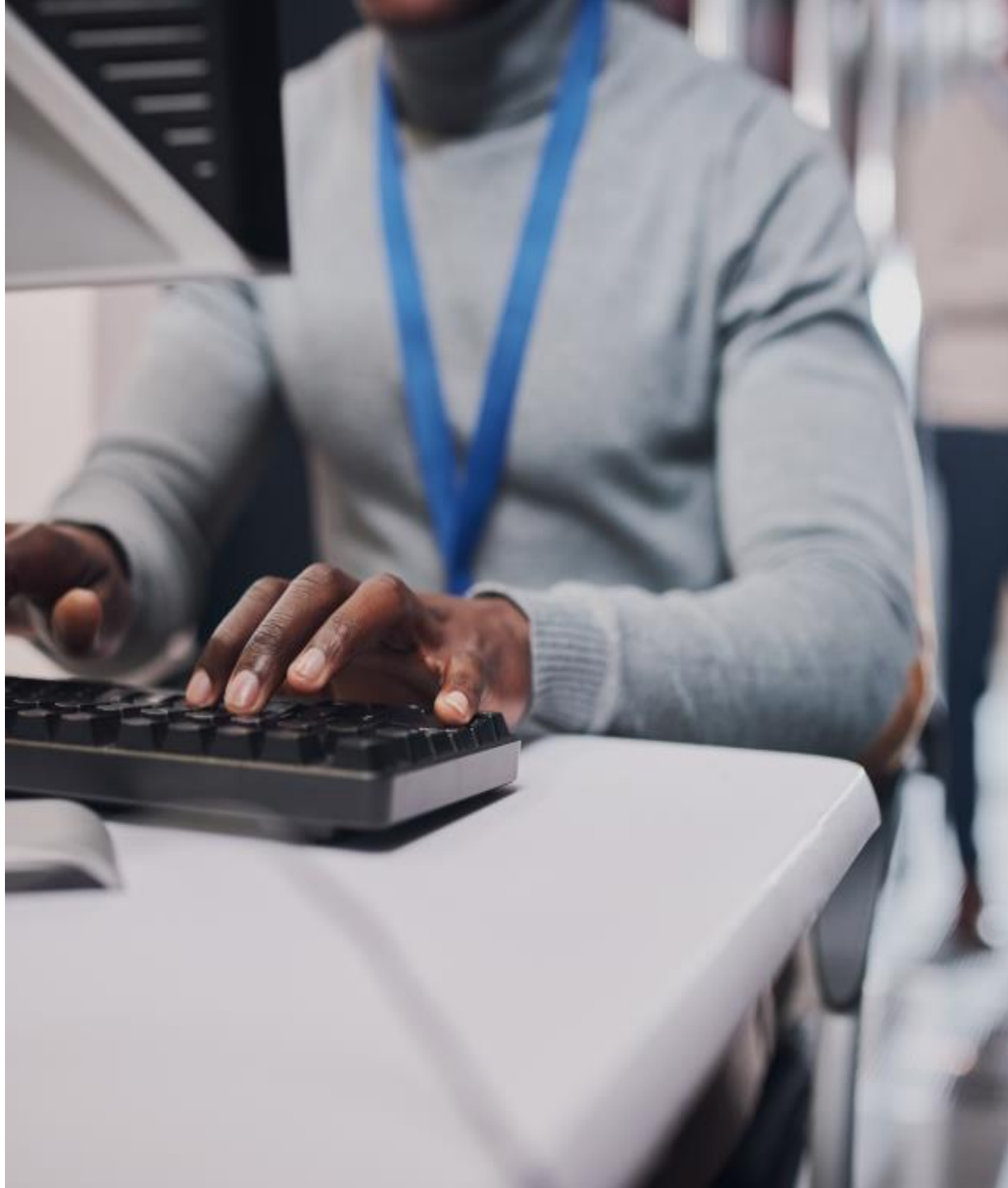
Leverage the global reach, scalability, know-how, and vigor of AWS to increase the customer base and find new opportunities

Grow

Join with AWS to improve the value of unique offerings with resources, programs, and benefits that lead to higher profits

AWS Support Center

- Customers must have permissions to access Support Center and to create a support case
- They can use one of the following options to access Support Center:
  - Use the email address and password associated with the AWS account, otherwise known as the AWS account root user
  - Use AWS Identity and Access Management (IAM)
  - Use the AWS Support API to access AWS Support and Trusted Advisor operations programmatically, if they have a Business, Enterprise On-Ramp, or Enterprise Support plan



AWS Knowledge Center

- The AWS Knowledge Center helps answer the questions most frequently asked by AWS Support customers and builders
- AWS security information is available from several areas for free
- Knowledge Center articles are available in ten languages:
  - Articles and videos are produced by an AWS team and display an "AWS OFFICIAL" badge

In this demo…

Use AWS Trusted Advisor, Health Dashboard, and Health API

Using AWS Trusted Advisor, Health Dashboard, and Health API

AWS Trust & Safety

- The AWS Trust & Safety (T&S) team is a global group that helps protect against abusive use of AWS services
- It also functions to build trust with AWS' customers, partners, and other stakeholders
- The T&S team scrutinizes potential abuse cases and contacts AWS customers to stop damaging activities
- The AWS T&S team serves as the first line of defense by investigating trends and reporting findings to AWS service groups as necessary

Governance at AWS

- AWS Governance is the capacity to introduce executive board policies and decisions that your cloud environment must observe
- This policy includes
  - The rules for the cloud environment
  - Definition of risks
  - Alignment with internal organizational policies

Governance at AWS

- Governance of the corporate environment is critical to understand why and how cloud services are consumed
- The cloud environment must align with the organization’s strategy on cloud service provider utilization
- All organizations, regardless of size and industry, need to establish a capability to effectively use cloud services, define policies and standards, understand and mitigate risks, and approve essential legal, commercial, and regulatory requirements

AWS Compliance Concepts

- AWS frequently attains third-party validation for thousands of global compliance requirements
- They continually monitor to help customers meet security and compliance standards for finance, retail, healthcare, government, and beyond
- Customers can inherit the latest security controls that AWS uses on its own infrastructure:
  - Customers can streamline and automate compliance and reporting

AWS Compliance Concepts

- AWS supports over 140 security standards and compliance certifications around the globe including:
  - Payment Card Industry Data Security Standard (PCI-DSS)
  - HIPAA/HITECH
  - Federal Risk and Authorization Management Program (FedRAMP)
  - General Data Protection Regulation (GDPR)
  - Federal Information Processing Standard 140-2 (FIPS 140-2)
  - National Institute of Standards and technology 800-171 (NIST 800-171)

Governance and Compliance Services

CloudWatch

Gathers and visualizes real-time logs, metrics, and event data in automated dashboards to streamline infrastructure and application maintenance

CloudTrail

Views, searches, downloads, archives, analyzes, and responds to API activity across the AWS infrastructure

AWS Audit Manager

Maps customer compliance requirements to AWS usage data with prebuilt and custom frameworks and automated evidence collection

AWS Config

Continually assesses, audits, and evaluates the configurations and relationships of AWS resources in on premises, and other clouds

AWS Artifact

- Artifact is a console-based, self-service auditing object retrieval service that gives customers quick and simple access to AWS compliance documentation and agreements
- Artifact **Agreements** enable customers to examine, approve, and manage agreements in AWS Organizations
- Artifact **reports** deliver compliance reports from third-party auditors who have tested and verified that AWS is compliant with a variety of global, regional, and industry-specific security standards and regulations

AWS Audit Manager

- Customers use AWS Audit Manager to continuously map their compliance requirements to AWS usage data with prebuilt and custom frameworks and automated evidence collection
- As the organization works to meet audit and regulatory obligations, they can save time by incorporating audit compliance processes into the DevOps model
- Audit Manager creates an HTTPS API endpoint to accomplish its solutions

Automating Compliance in the Cloud

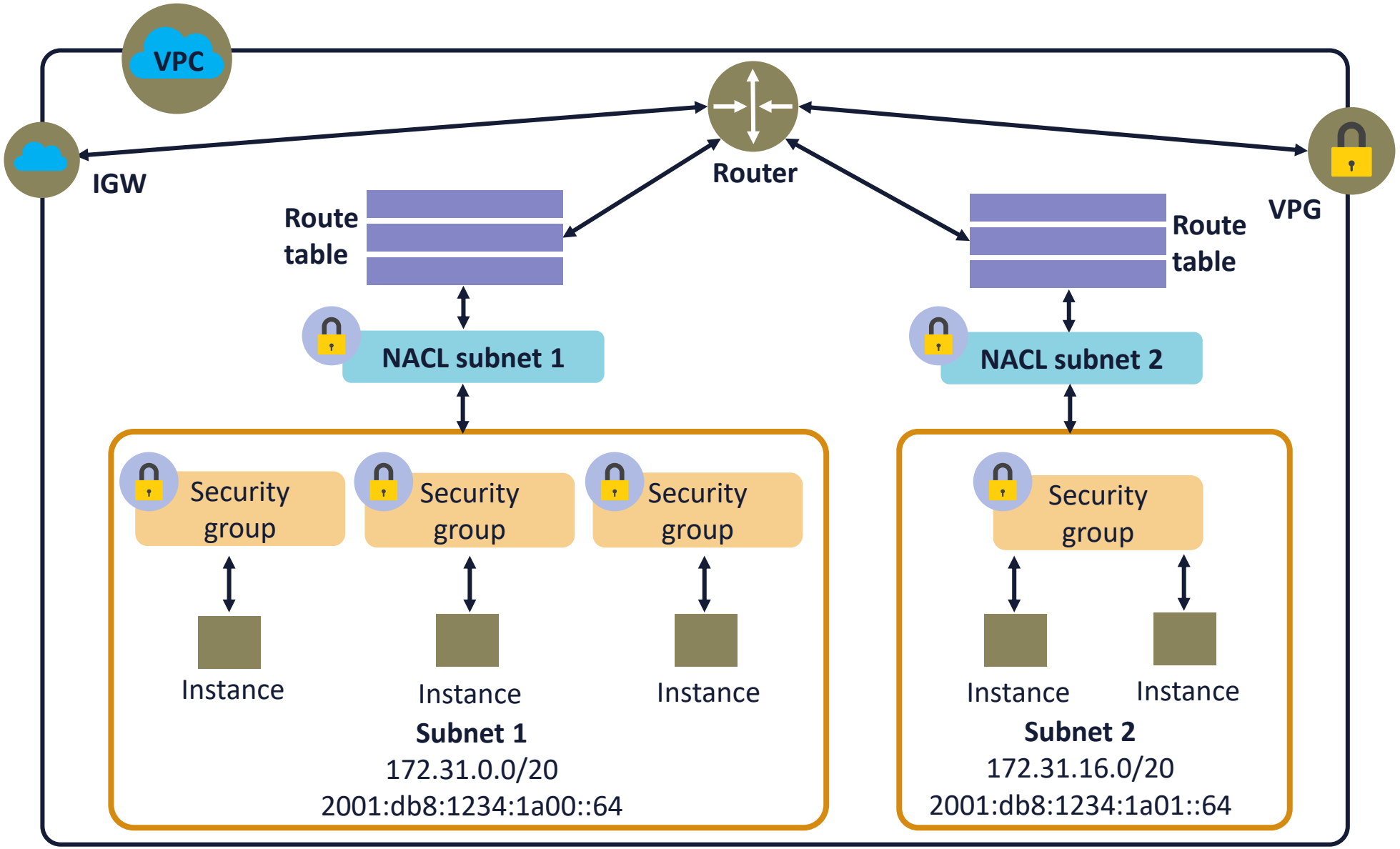
- By introducing compliance requirements early in the product or service life cycle, customers can ensure that they address policy and regulation objectives while improving the value proposition
- Automating compliance in the cloud has three benefits:
  - There is an immediate cost savings
  - Shifting workloads to the cloud logically encourages greater automation
  - When the automated process identifies a problem, the remediation can be much easier to deploy

Using the Well-Architected Framework

In this demo…

Use the Well-Architected Framework at the AWS website

Virtual Private Cloud (VPC) Begins With Design



Examining Components of a VPC

In this demo…

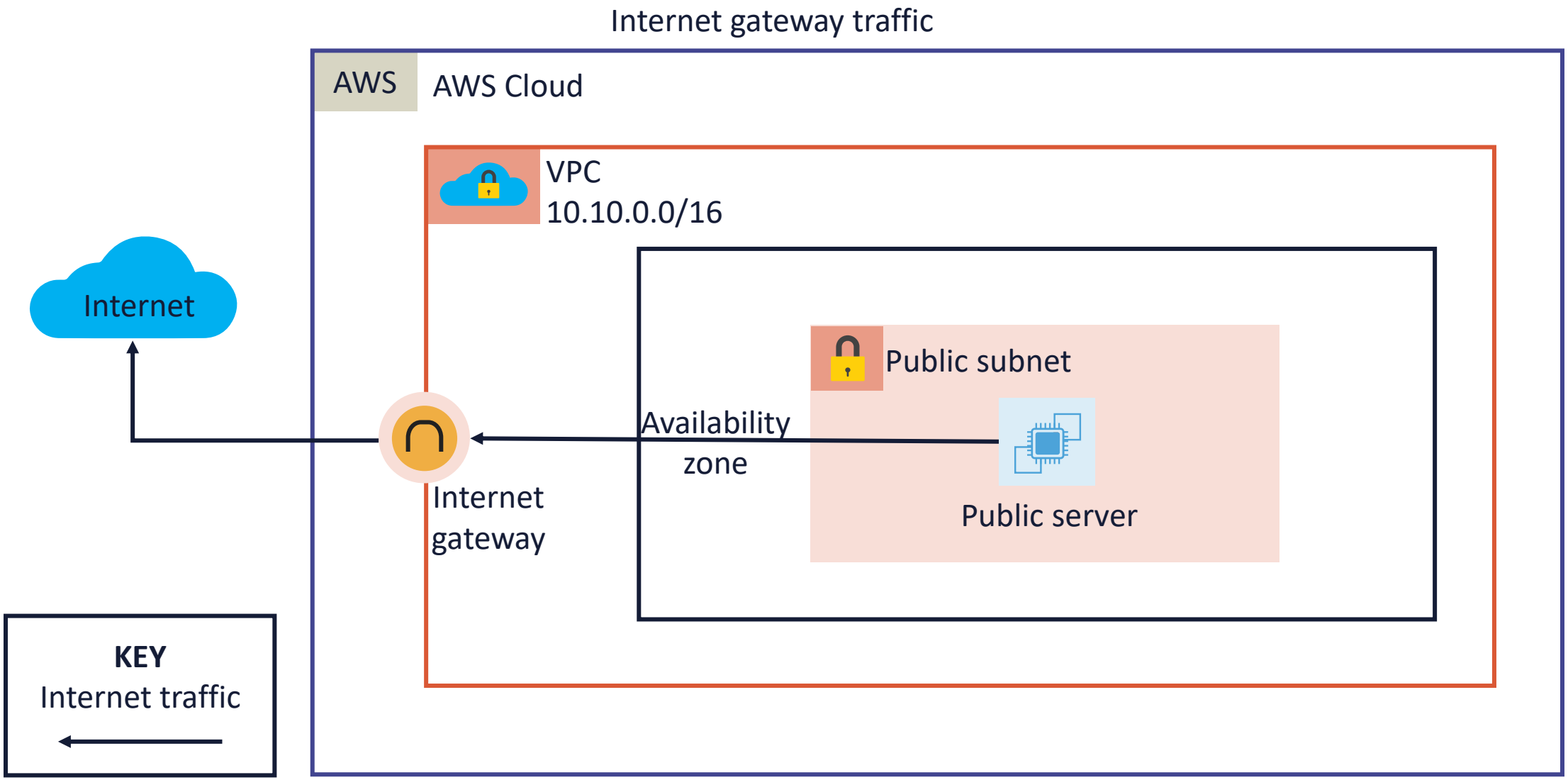
Examine the basic components of my sample default VPC

Common VPC Addressing

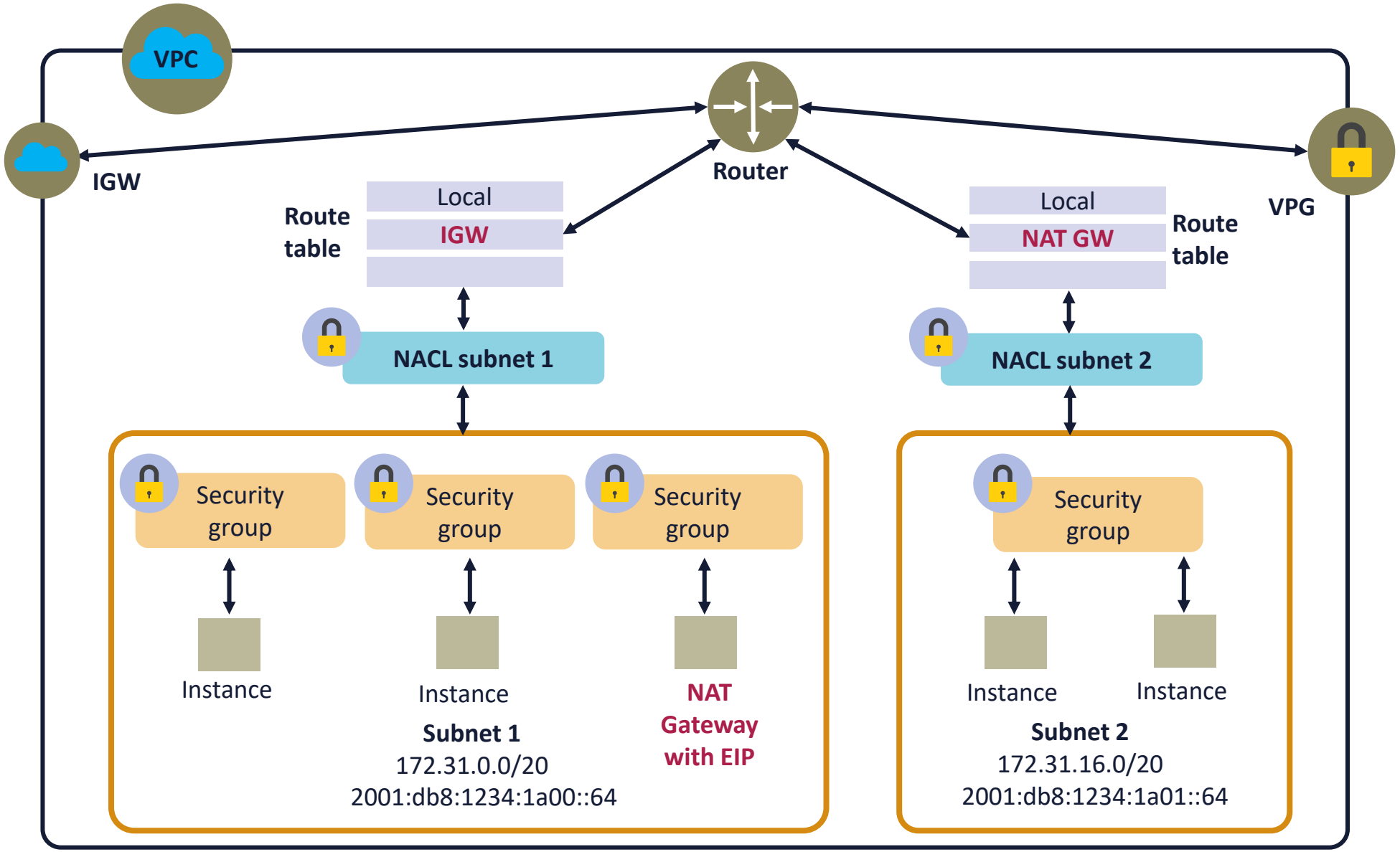
- Default VPC CIDR prefix is 172.16.0.0/16 (Don’t use 172.17.0.0)
- Default subnets are /20 that provides 4089 hosts
- Need ~ 2000 hosts? Use a /21 CIDR
- Need ~ 1000 hosts? Use a /22 CIDR
- Need ~ 500 hosts? Use a /23 CIDR
- Need ~ 250 hosts? Use a /24 CIDR

- All IPv6 hosts have a /64 CIDR

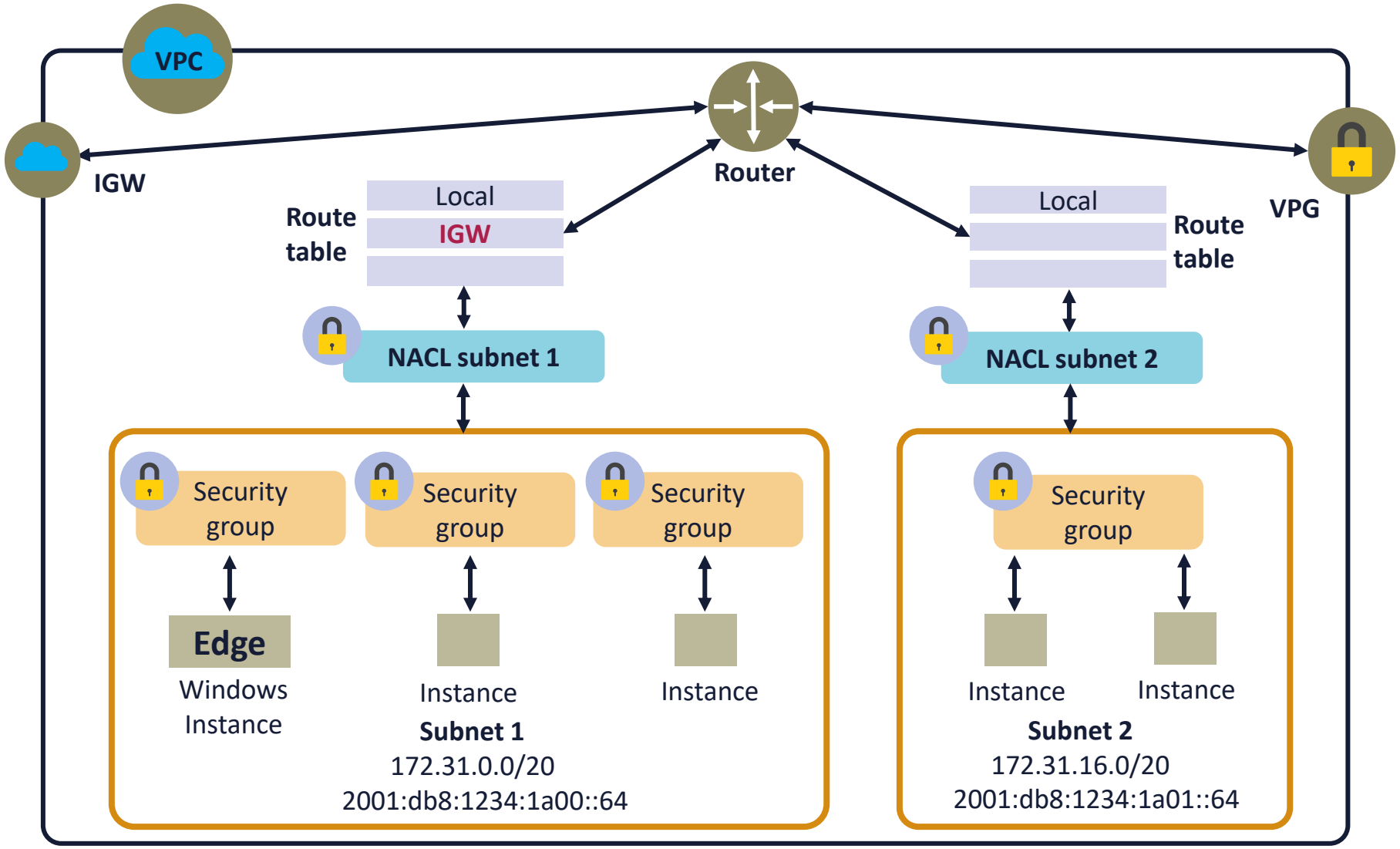
Connecting to AWS Through an Internet Gateway



NAT Gateways



Interface Endpoints



EFS

S3

Comparing Endpoints and Endpoint Services

In this demo…

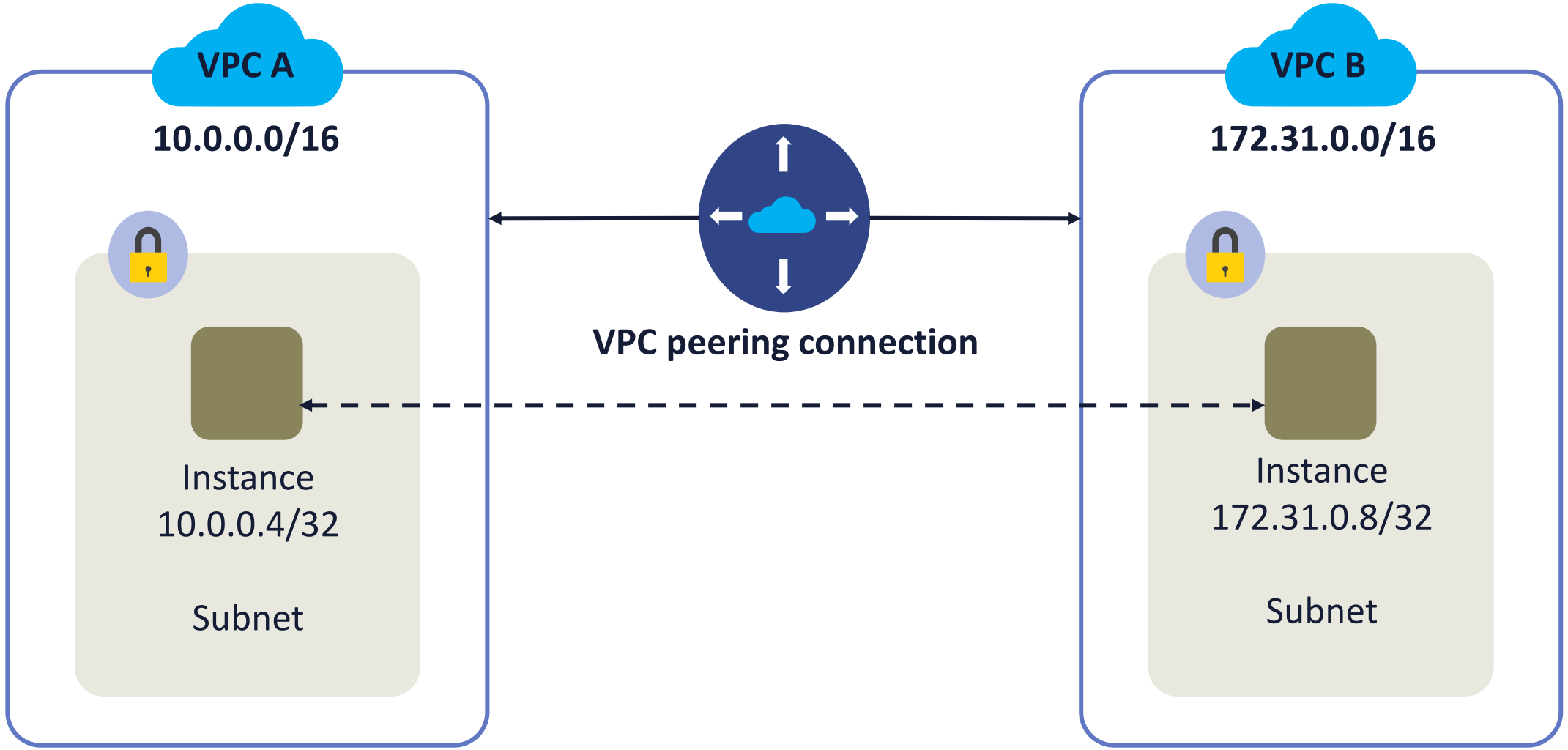
Compare:

- Endpoint Services: PrivateLink
- https://aws.amazon.com/privatelink/

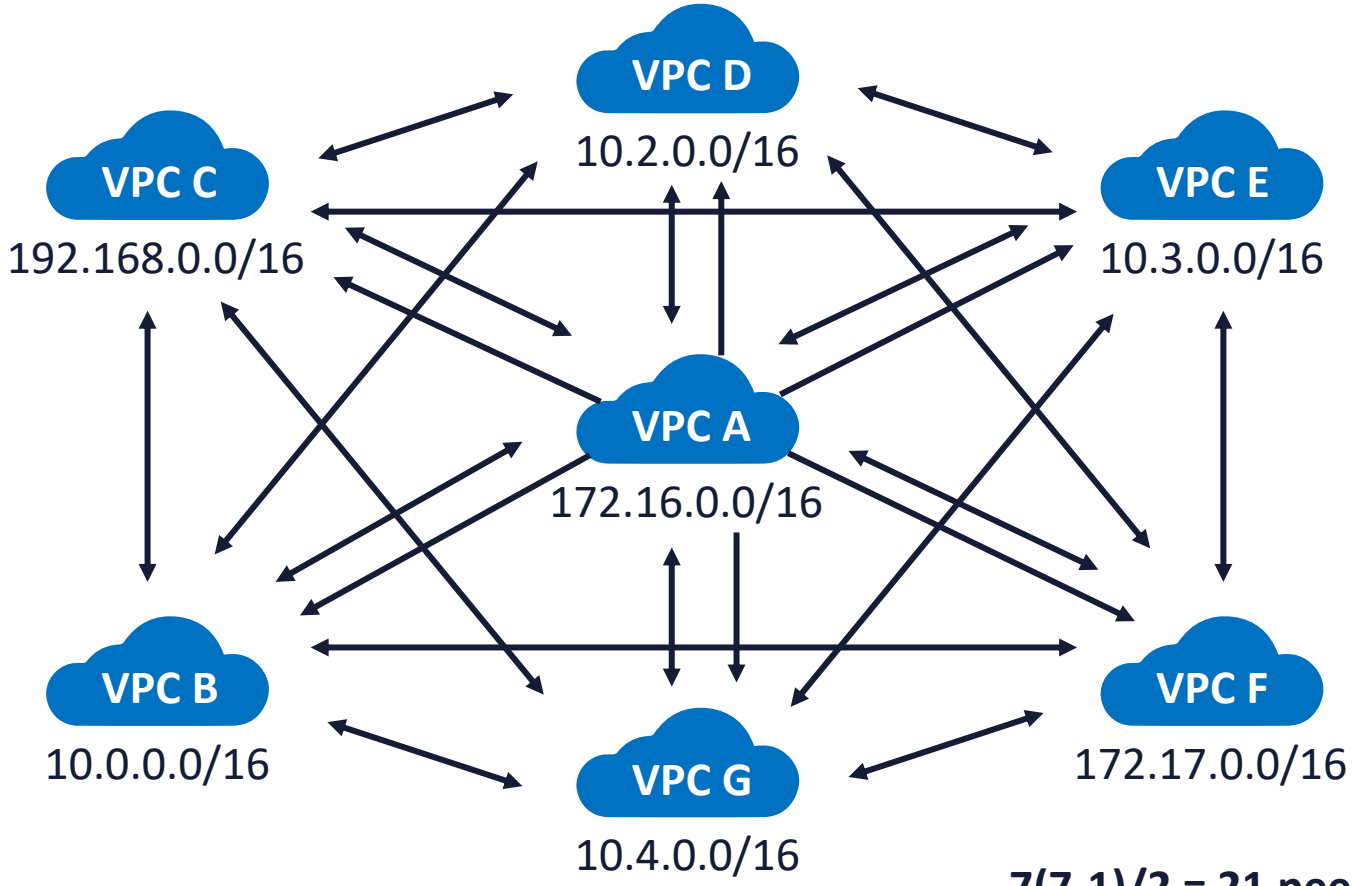
VPC Peering

- A VPC peering connection is a networking connection between two VPCs
- Customers can route traffic between them using private IPv4 or IPv6 addresses:
  - Instances in either VPC can communicate with each other as if they are within the same network
- VPC peering connections can be between your own VPCs or with a VPC in another AWS account
- Intra-region or inter-region peering connections are allowed

VPC Peering


VPC A
10.0.0.0/16
VPC B
172.31.0.0/16
VPC peering connection
Instance
10.0.0.4/32
Subnet
Instance
172.31.0.8/32
Subnet

VPC Full-Mesh Peering

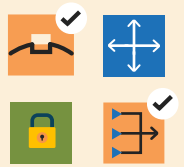


7(7-1)/2 = 21 peering connections

VPC peering connection

AWS Resource Access Manager (AWS RAM)

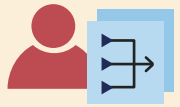
AWS Resource Access Manager
Manage access to resources by creating a resource share



Specify resource share details
Select the resource share details, like name and resource type, and assign to resources

Associate permissions
Choose which actions can be performed on each resource type in the resource share

Grant access to principals
Specify organizational unit (OU), AWS account(s), IAM role and users

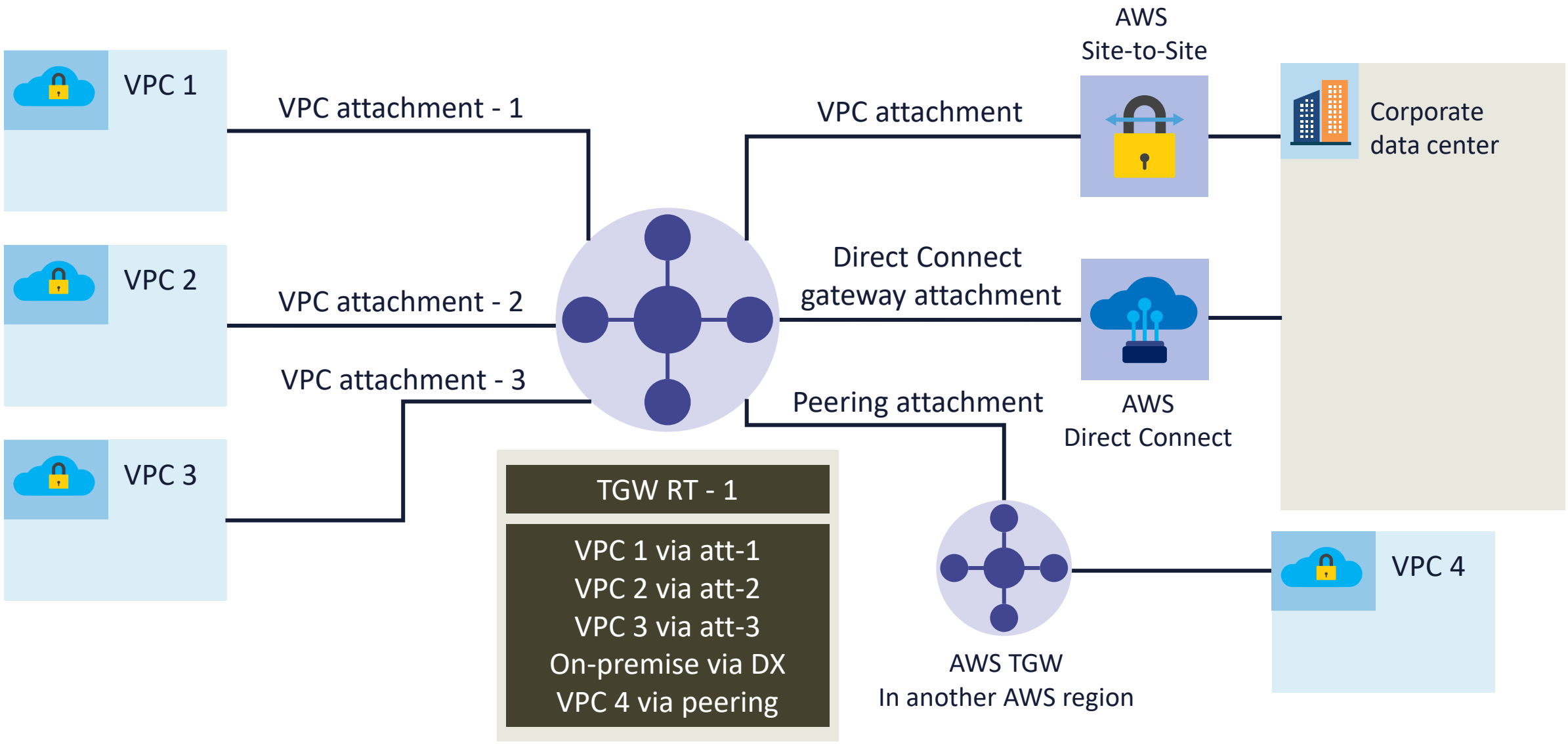


Review and create
The resources will now be accessible according to the specified permissions

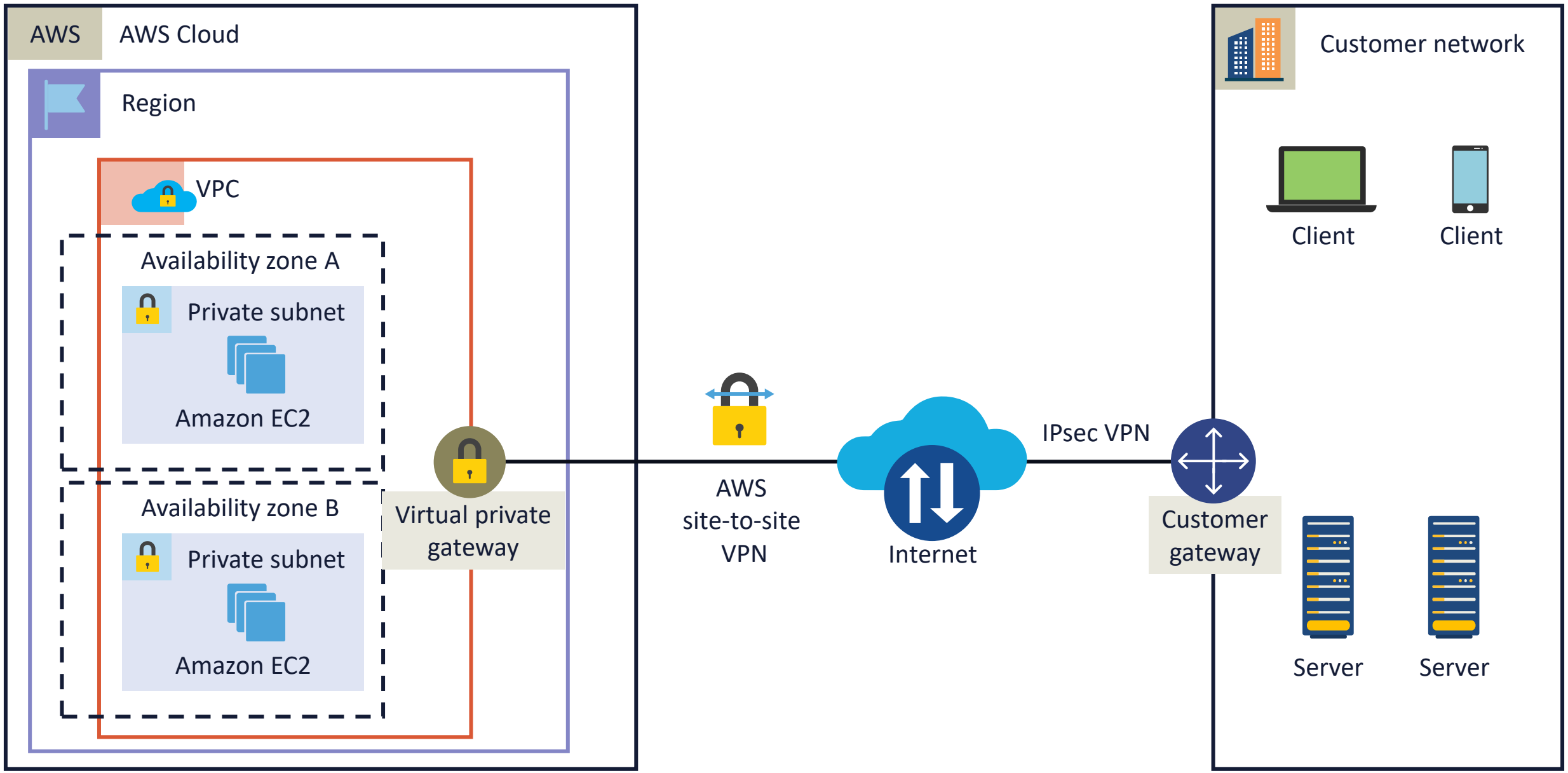
Transit Gateway

- AWS Transit Gateway is a centralized logical routed hub entity that allows customers to connect their VPCs and their on-premises networks to a single gateway
- It is an AWS managed high availability and scalability regional network transit hub used to interconnect VPCs and customer networks
- Transit Gateway is a region-specific virtual router that acts as a hub, controlling how traffic is routed among all the connected networks – basically between hundreds of VPCs and your on-premise network:
  - Up to 5000 VPCs can be attached to a single gateway with 10,000 routes limit

AWS Transit Gateway



Connecting to AWS Through a Site-to-Site VPN



Exploring Network Connectivity Options

In this demo…

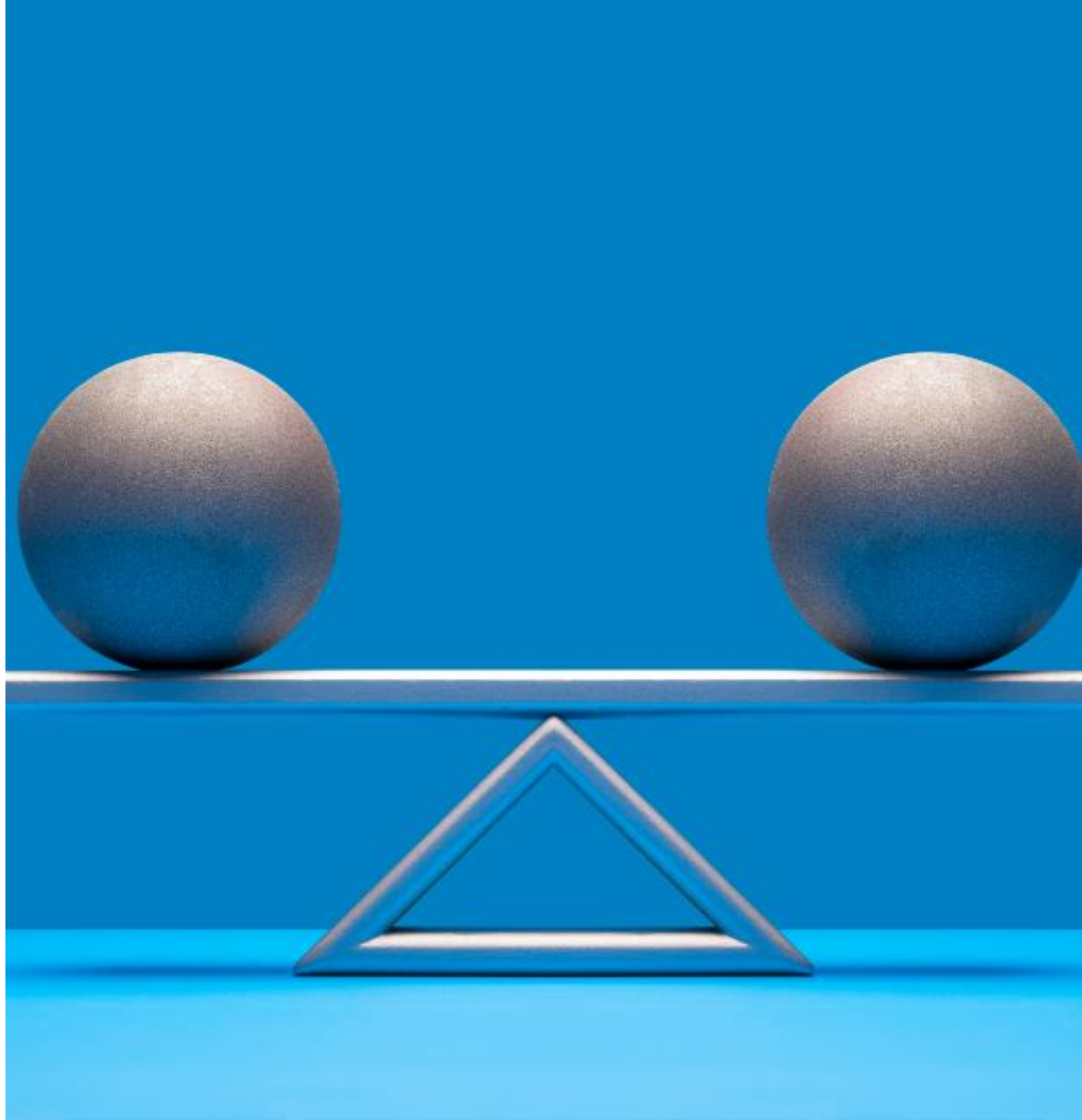
Explore AWS Site-to-Site (Managed) VPN

AWS Certificate Manager (ACM)

- AWS customers can leverage the AWS Certificate Manager (ACM) to provision, manage, and deploy public and private TLS certificates for use with AWS services and even internal connected resources
- ACM removes the time-consuming manual process of acquiring, loading, and renewing TLS certificates:
  - Domain-validated public certificates
  - Private certificates from AWS Private CA
  - Imported public or private certificates

AWS Load Balancing

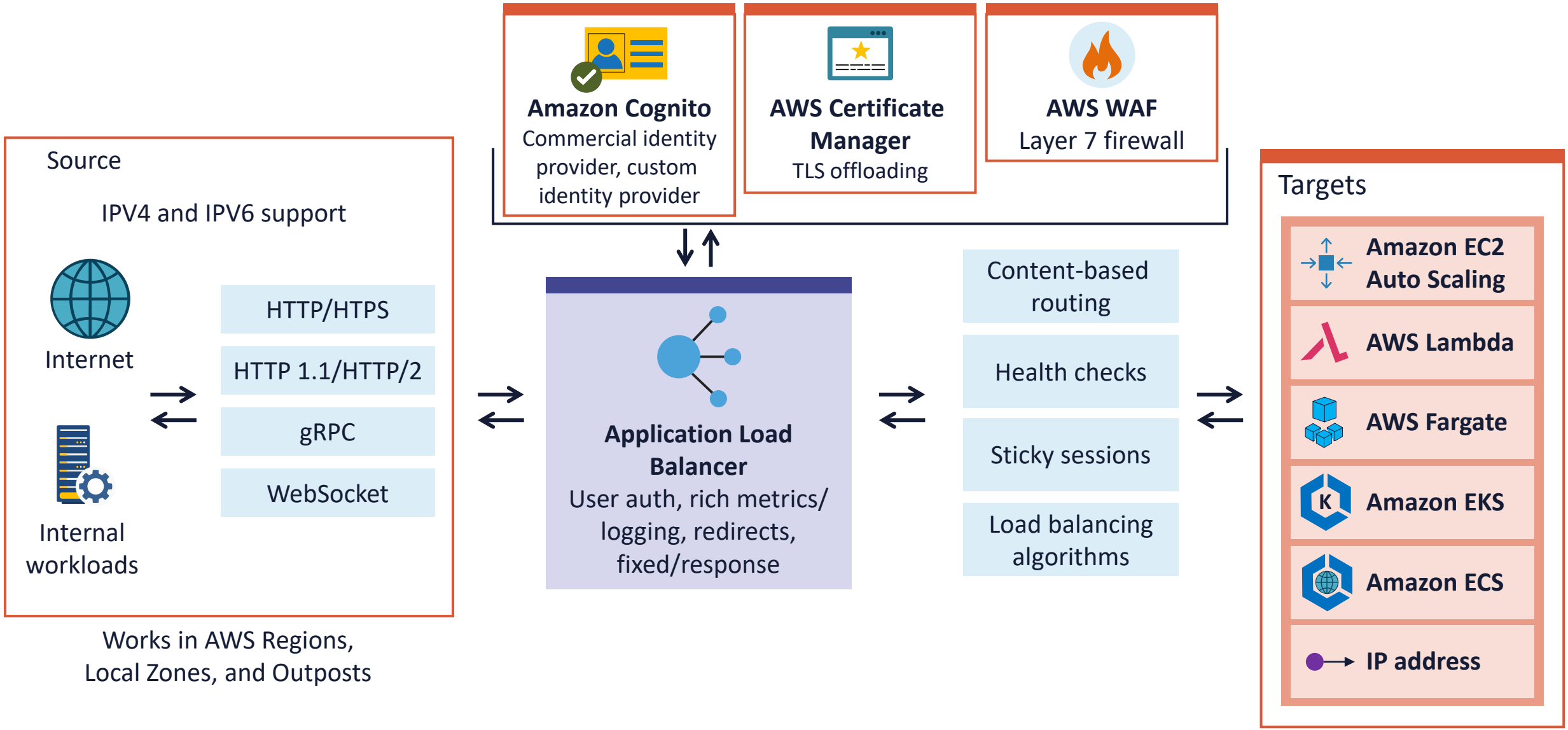
- Load balancing is a technique for allocating network traffic equally across a pool of resources that host an application
- Modern applications must process millions of users at the same time and respond with the requested files, videos, images, and other data in a rapid and reliable way
- To accommodate high amounts of traffic, most applications have numerous resource servers that transfer data between them



AWS Load Balancing

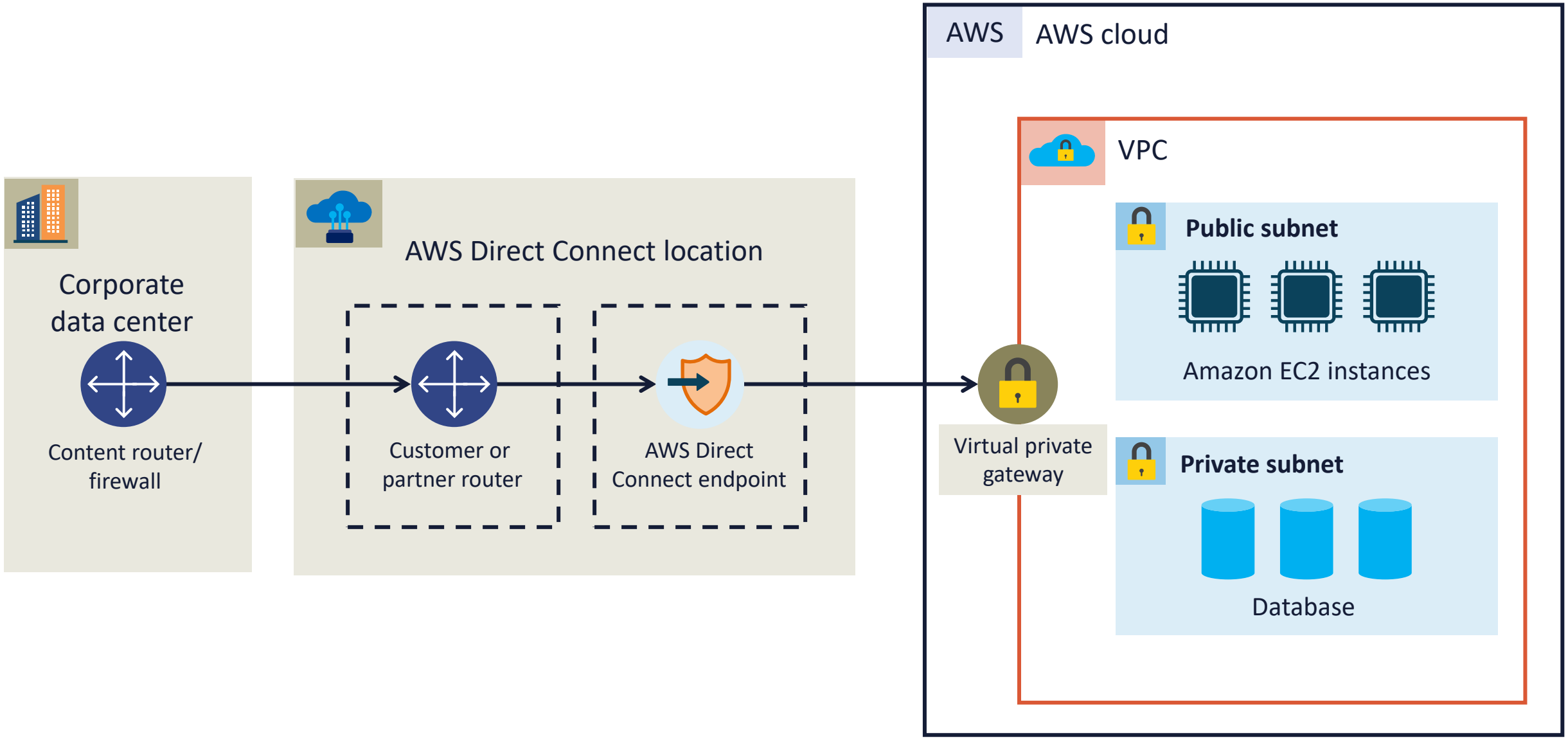
- A load balancer is a device that is placed between the client and the server group and functions as a transparent mediator
- It ensures that all resource servers are leveraged equally by providing
  - Scalability
  - Security
  - Performance

AWS Application Load Balancer



Works in AWS Regions, Local Zones, and Outposts

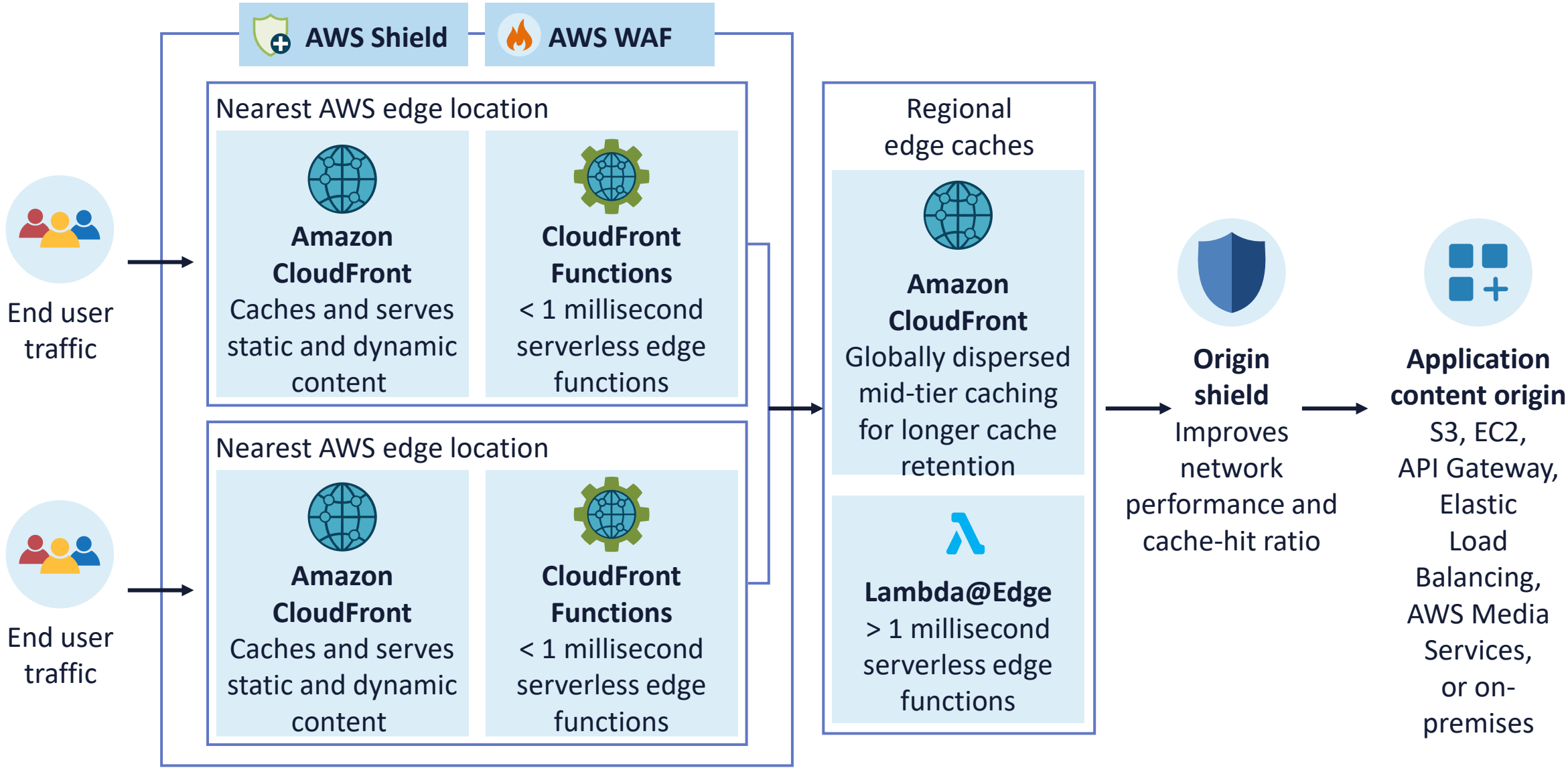
Connecting to AWS Through Direct Connect and a VPC



Edge Network Services: Amazon Cloudfront

- Is a content delivery network (CDN) service designed for high performance, security, and developer suitability
- Securely delivers data, videos, applications, and application programming interfaces (APIs) to customers globally with low latency and high transfer speeds within a developer-friendly environment
- Is integrated with AWS – both physical locations that are directly connected to the AWS global edge locations and various service endpoints

Amazon Cloudfront

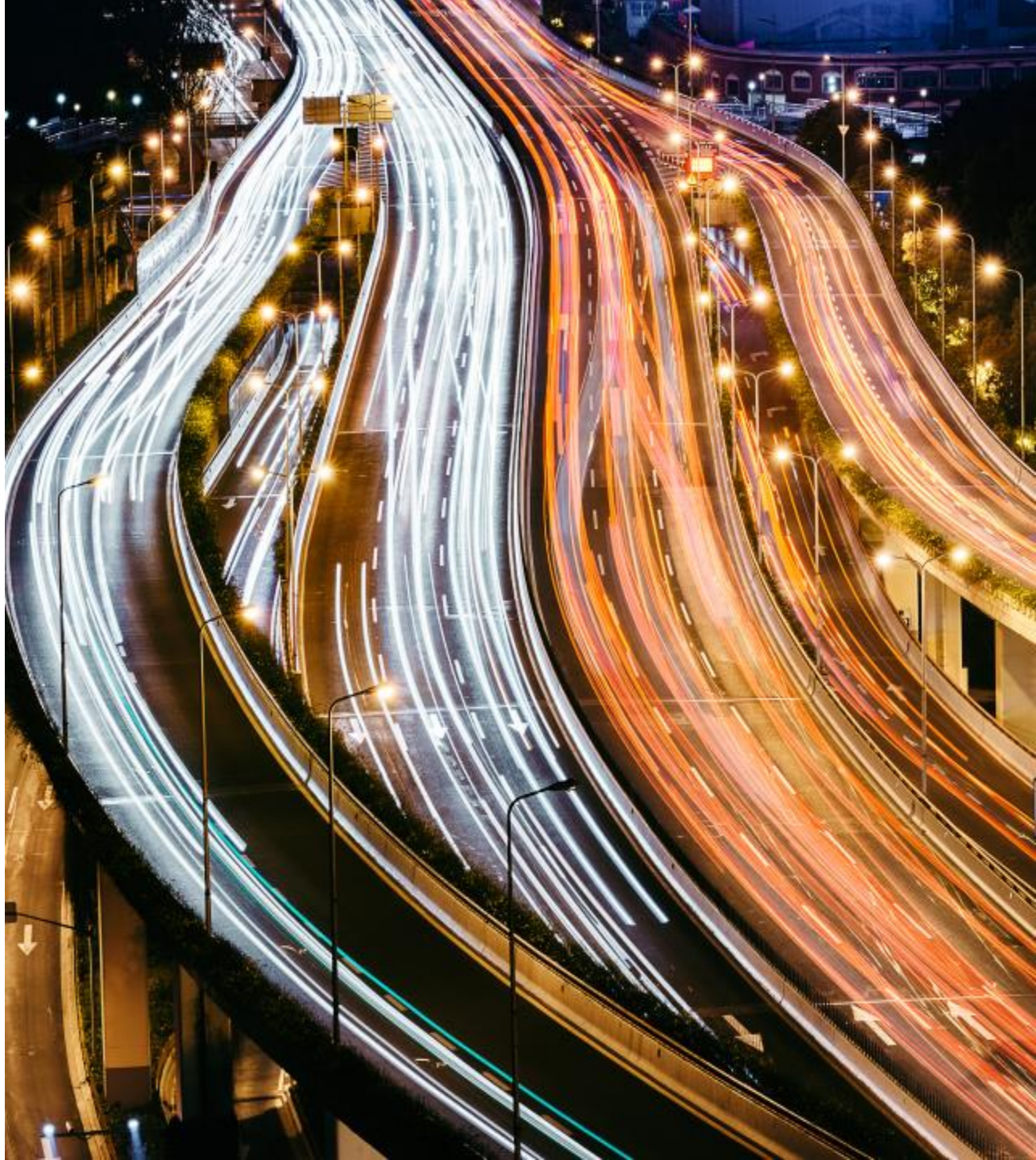


Edge Locations

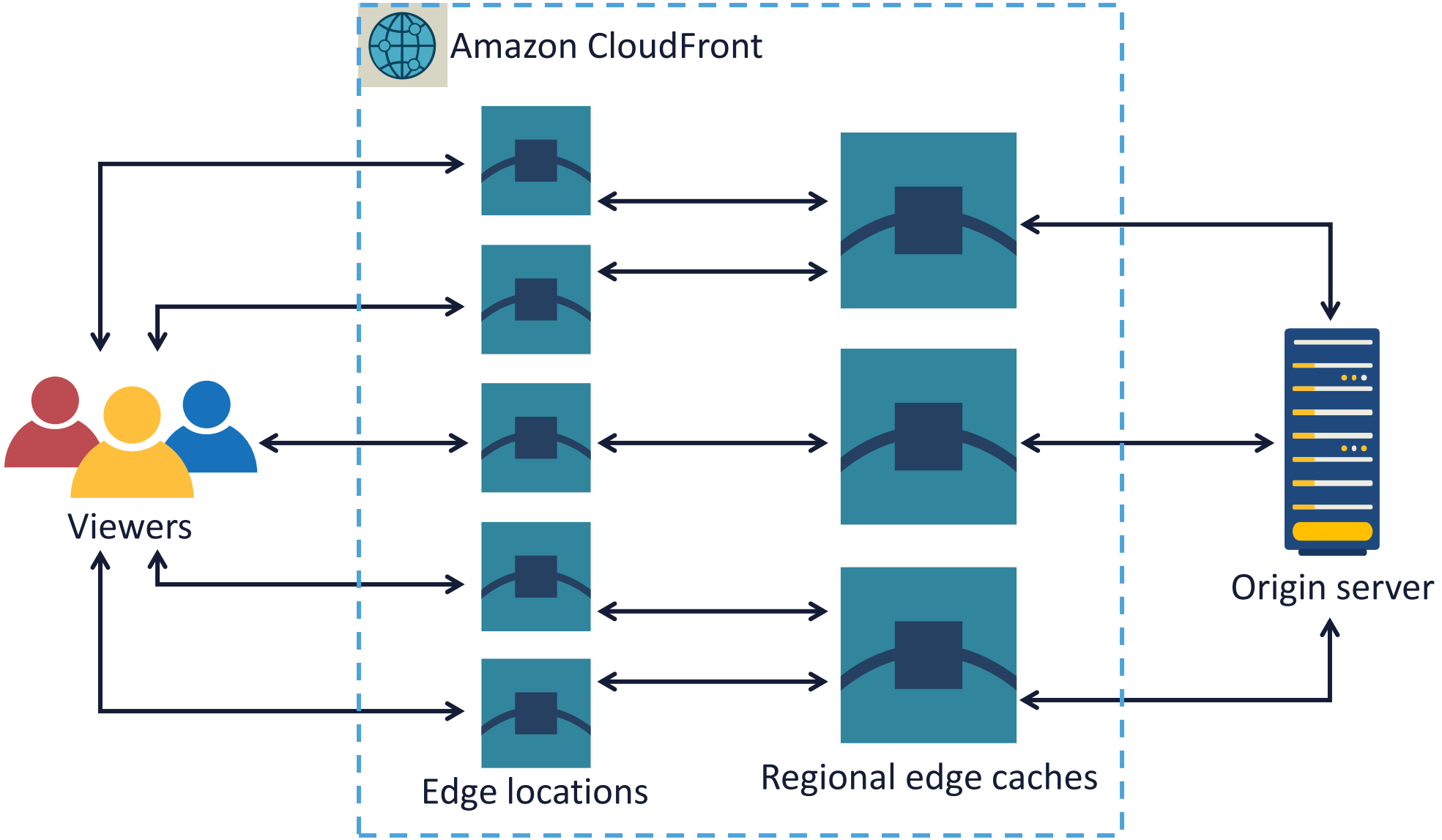
- Edge locations are AWS data centers and metropolitan area partners that are designed to deliver customer services with the lowest possible latency
- Amazon has dozens of these data centers spread across the world
- They are closer to users than regions or AZs, often in major cities, so responses can be extremely fast

Benefits of Edge Locations

- Amazon CloudFront (CDN) uses edge locations to cache copies of the content that it serves, presenting it closer to consumers and delivering to them faster
- Route 53 serves DNS responses from edge locations so that DNS queries that originate nearby can resolve faster
- Web application firewall (WAF) and AWS Shield (Standard and Advanced) filter traffic in edge locations to stop unwanted traffic as soon as possible



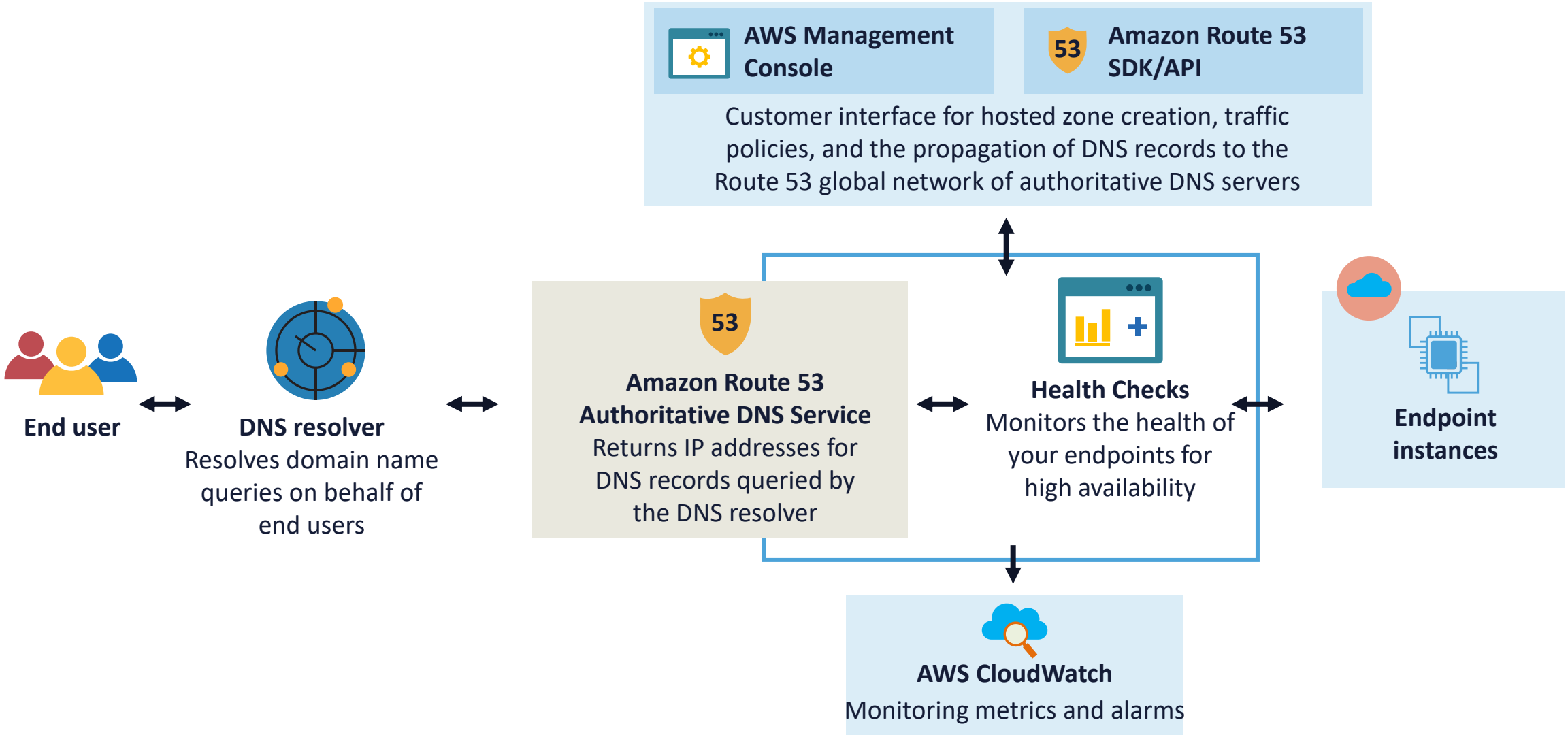
AWS Edge Locations



Amazon Route 53

- Is a highly available and scalable cloud domain name system (DNS) web service
- Is designed to offer a very dependable and cost-effective method to route end users to Internet applications by translating human-readable names to IPv4 and IPv6 addresses
- Effectively connects user requests to AWS services like EC2 instances, Elastic Load Balancing load balancers, and Simple Storage Service (S3) buckets
- Can also be used to route users to infrastructure outside of AWS

Amazon Route 53



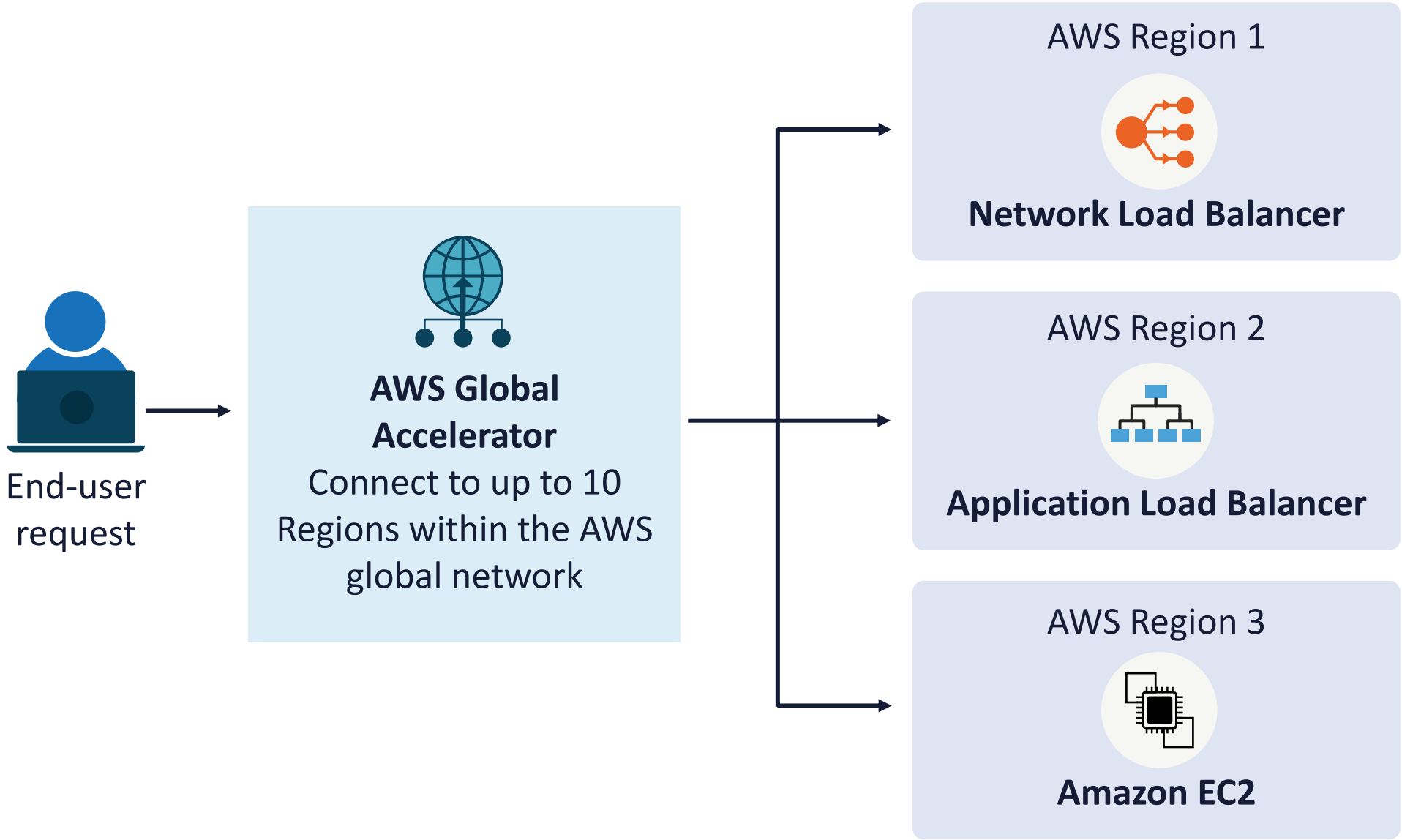
Edge Network Services: Global Accelerator

- Is a robust networking service that enables customers to expand the availability, performance, and security of their public applications
- Offers two global static public IPs that represent a fixed entry point to application endpoints such as Application Load Balancers, Network Load Balancers, Amazon Elastic Compute Cloud (EC2) instances, and elastic IPs

Global Accelerator Use Cases

- Use traffic dials as a global traffic manager to route traffic to the nearest region or attain fast failover across multiple regions
- Accelerate API workloads by up to 60%, leveraging TCP termination at the edge
- Simplify allowlisting in enterprise firewalling and IoT scenarios using global static IPs
- Use custom routing to deterministically route traffic to a fleet of EC2 instances for low-latency gaming and media

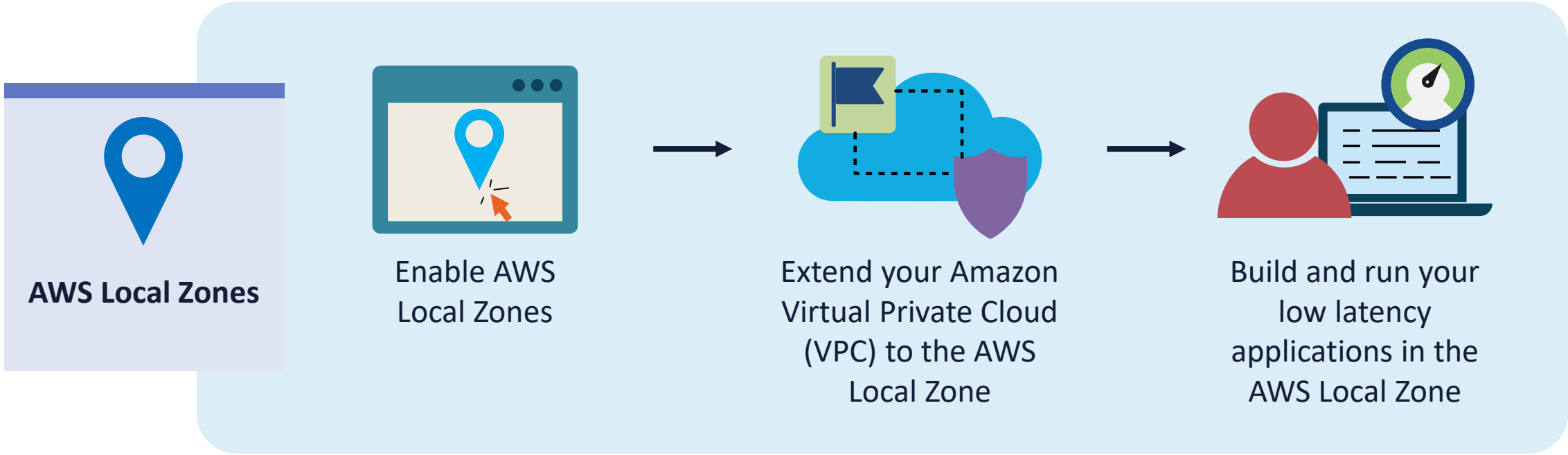
Global Accelerator



AWS Local Zones

- Local Zones are an infrastructure deployment solution that places compute, storage, database, and other specific AWS services close to large population and industry centers
- AWS customers often migrate their applications to a nearby AWS Local Zone while still addressing the low-latency needs of hybrid deployment
- Local Zones enable
  - Real-time gaming
  - Live streaming
  - Augmented and virtual reality (AR/VR)
  - Virtual workstations, and more

AWS Local Zones



AWS Outposts

- Outposts is a collection of fully managed solutions that deliver AWS infrastructure and services to most on-premises or edge locations for a reliable hybrid cloud experience
- With AWS Outposts, customers can run some AWS services on-premises and connect to a wide array of services available in the local AWS Region
- They can run applications and workloads on-premises using familiar AWS services, tools, and APIs

AWS Outposts

- AWS Outposts supports workloads and devices needing low latency access to on-premises systems, local data processing, data residency, and application migration initiatives with local system interdependencies
- It is available in a variety of form factors, including racks and multiple rack environments:
  - The AWS Outposts rack is an industry-standard 42U form factor
  - The AWS Outposts servers come in a 1U or 2U form factor

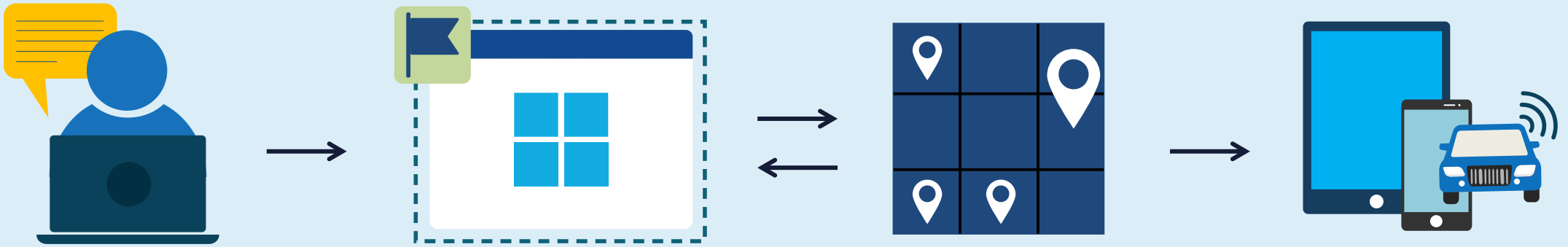
AWS Outposts Use Cases

- **Low latency compute** – provide high-quality gaming environments for interactive applications, like real-time multiplayer games across the world
- **Data residency** – data often must remain in a specific country, state, or province for regulatory, contractual, or data security initiatives
- **Migration and modernization** – legacy on-premises applications can have latency-sensitive system dependencies, making them problematic to migrate
- **Local data processing** – process data locally for use cases like data lakes and machine learning (ML) model training or to provide a reliable hybrid architecture

AWS Wavelength

- AWS Wavelength inserts AWS compute and storage services into 5G networks
- It offers a mobile edge computing infrastructure for developing, deploying, and scaling ultra-low-latency applications
- Customers often use this to deliver high-resolution live video streaming, high-fidelity audio, and AR/VR applications using 5G cellular
- Another use case is to run AI and ML video and image analytics at the edge to accelerate 5G systems in retail, medical diagnostics, and more

AWS Wavelength Zones



Extend the Amazon VPC to include a Wavelength Zone and then create AWS resources like Amazon EC2 instances in the desired subnets

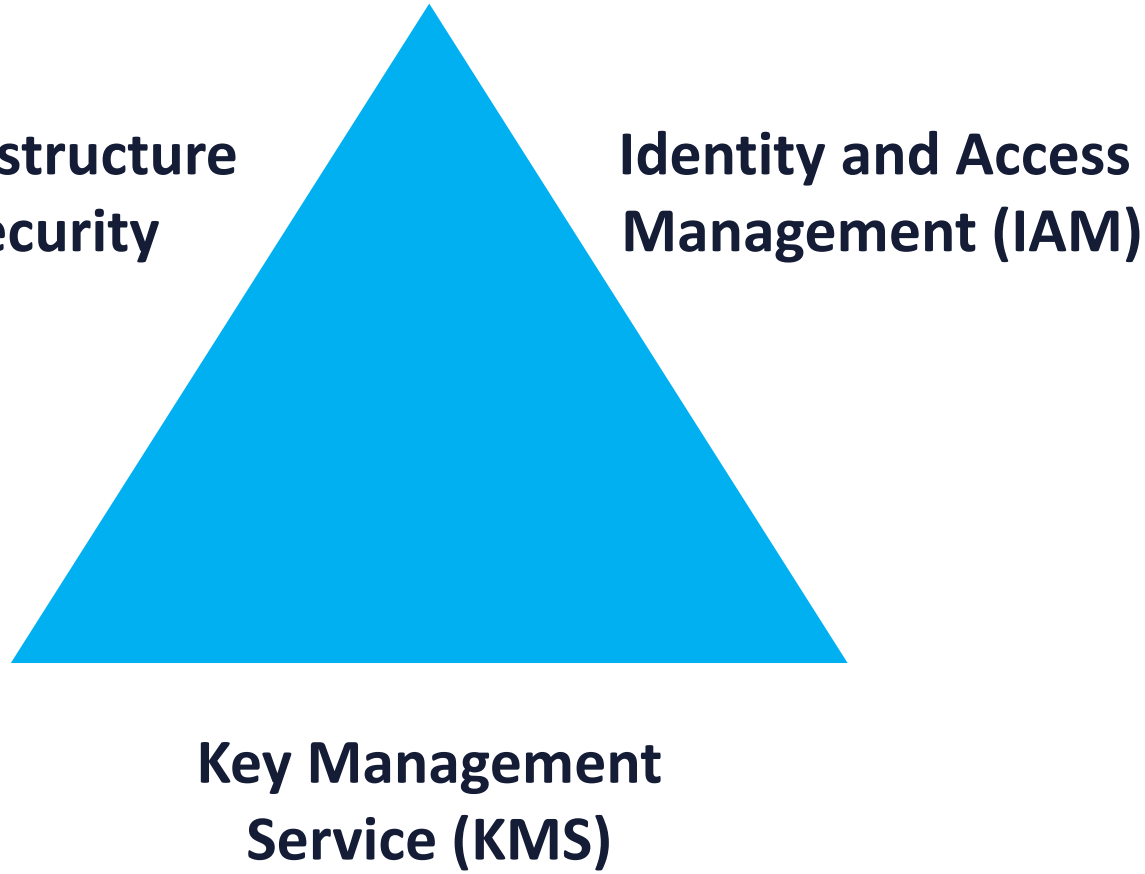
AWS Region

Wavelength Zone

Deploy the portions of an application that require ultra-low latency in a Wavelength Zone, and then seamlessly connect back to the rest of the application and the full range of cloud services running in the AWS Region

Application traffic can reach application servers running in Wavelength Zones without leaving the mobile network

AWS Security Triad



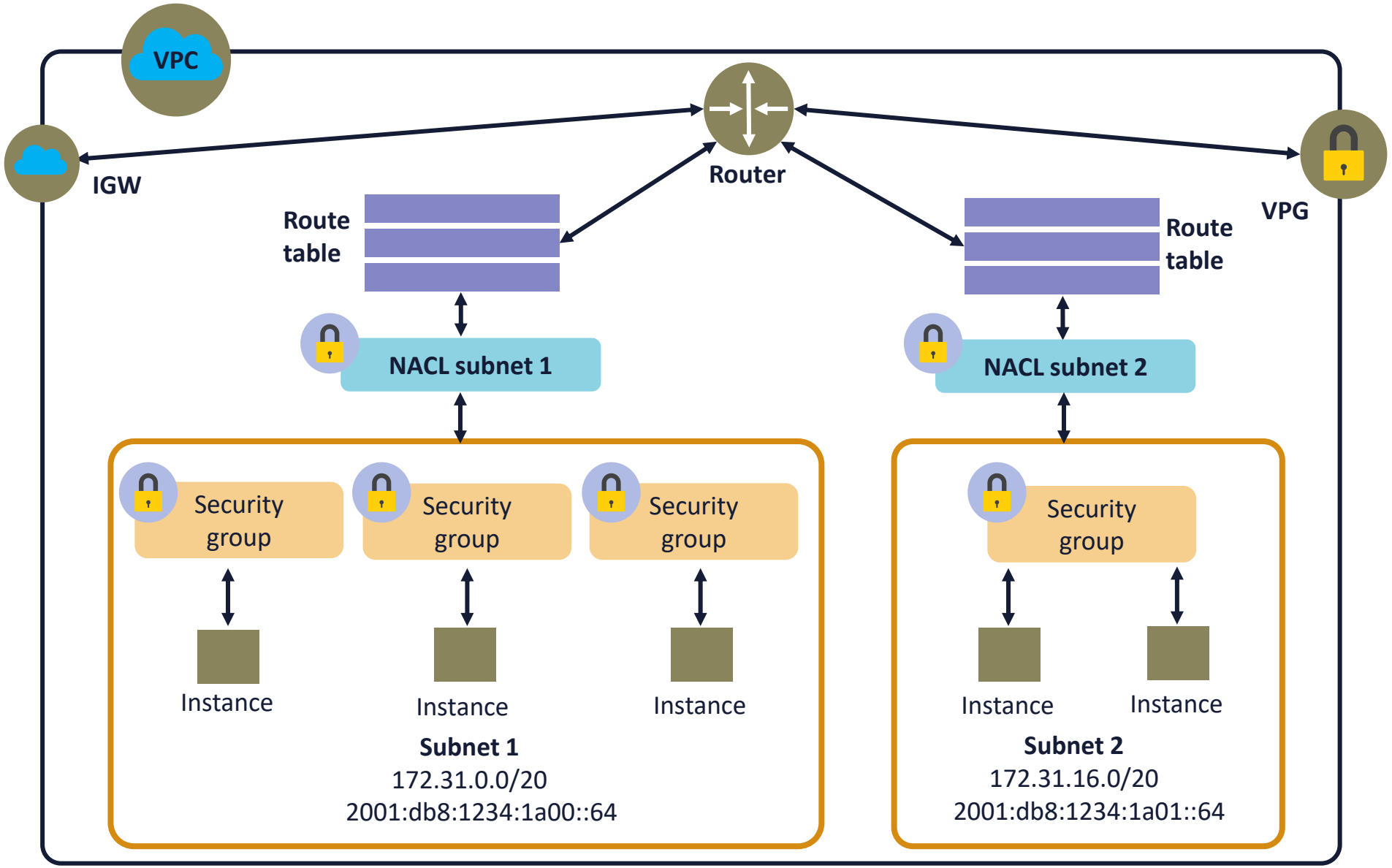
Network Access Control Lists (NACLS)

- Allow stateless traffic filtering to all inbound or outbound traffic on a VPC subnet
- Apply to all instances and appliances in the associated subnet
- Typically contain ordered rules to permit or deny traffic:
  - Rules are processed with a numbered order

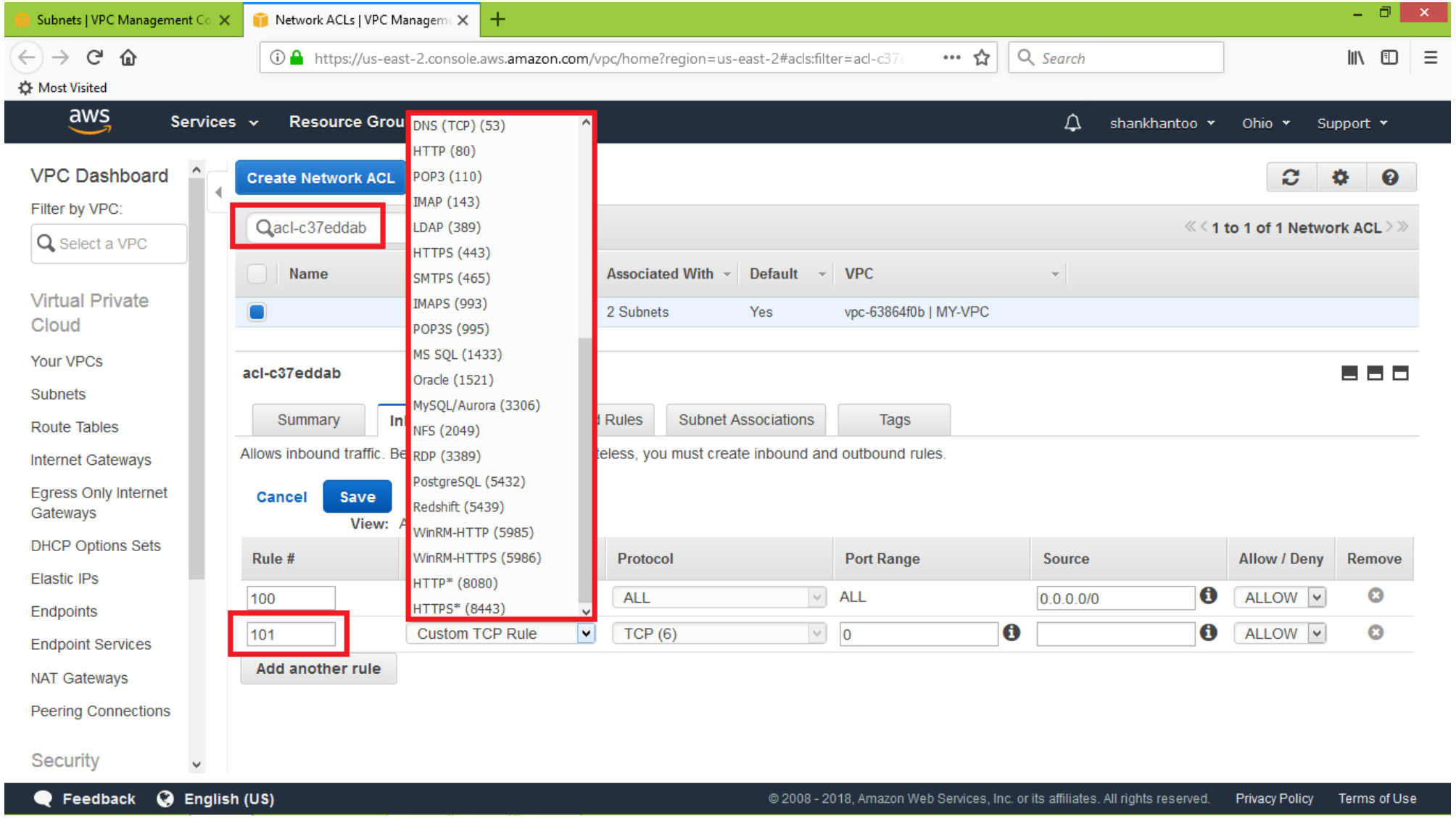
Network ACLs (NACLs)

- A NACL is agnostic of Transmission Control Protocol (TCP) connections or User Datagram Protocol (UDP)/Internet Control Message Protocol (ICMP) flows
- They are stateless (static) in that the return traffic must be explicitly allowed in the inbound NACL
- These firewalls work together with security groups and can permit or deny traffic before it reaches the interfaces

Network ACLs



Network ACLs



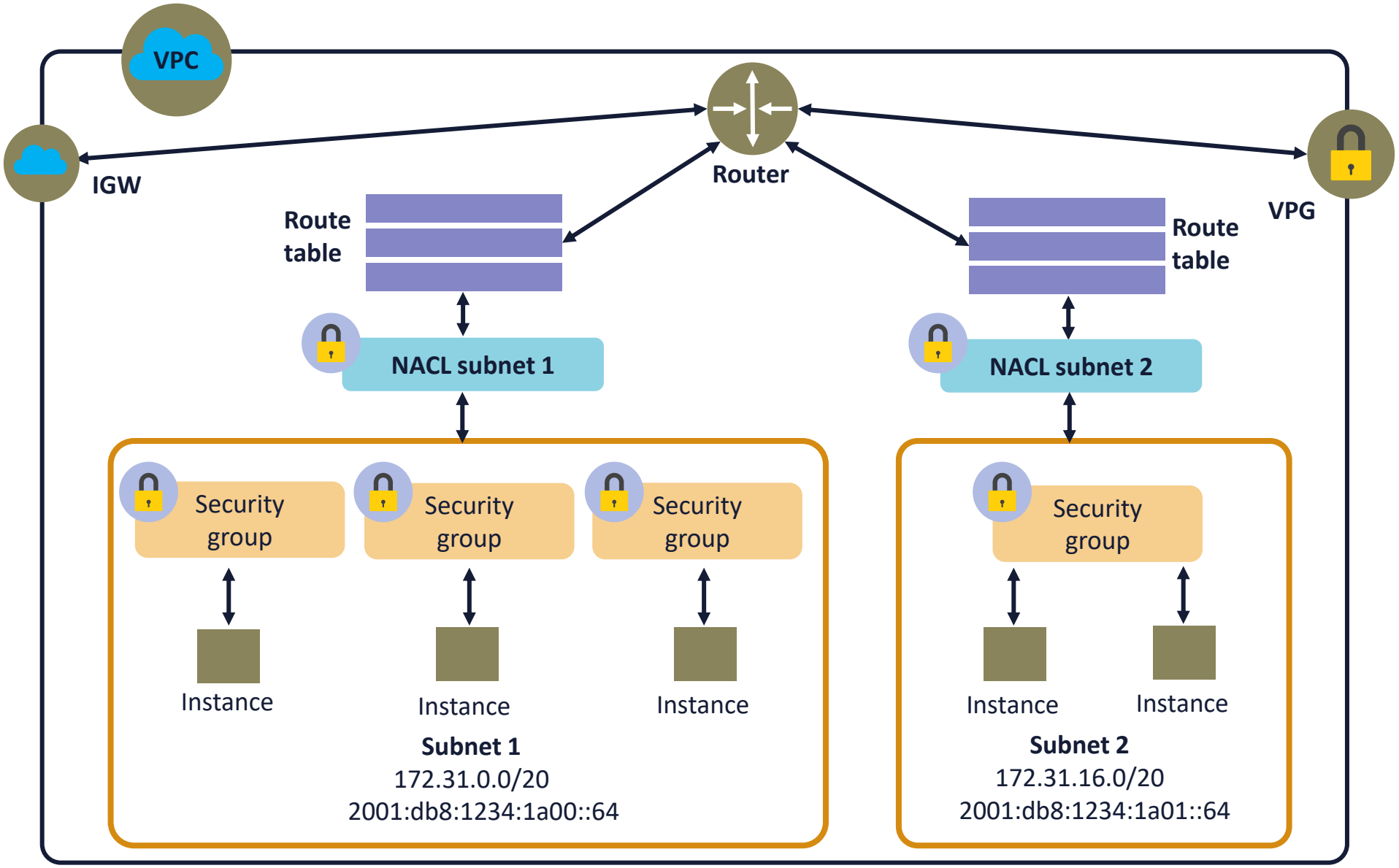
Security Groups

- Security group (SG) firewalls apply to individual Elastic Compute Cloud (EC2) instances in a subnet
- They operate at the hypervisor level attached to the virtual elastic network interfaces (eth0)
- SGs are layer 3/4 stateful virtual "Allow Only" firewalls
- They have no explicit deny rules like NACLs
- ALL EC2 instances are launched with the default SG unless otherwise designated
- All rules in all applied SGs are evaluated before a decision is made

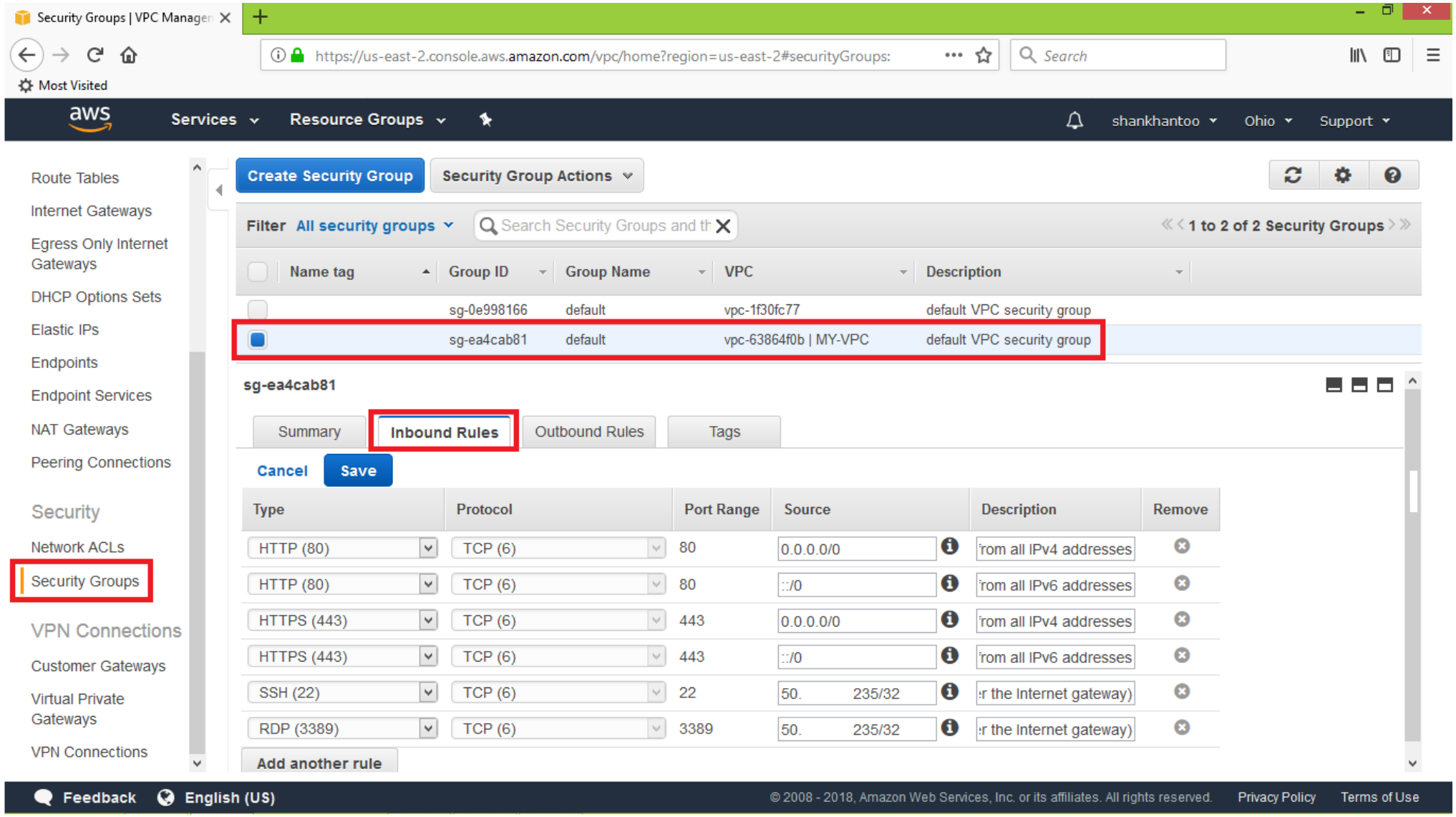
Security Groups

- An unchanged default SG will allow communication between all resources within the security group AND all outbound traffic – all other traffic is implicitly denied:
  - Return traffic is automatically allowed (with Shield Standard inspection)
- There are no limits (quotas) on the number of SGs per VPC, on the number of rules you can add to a security group, and on the number of SGs that you can use with an elastic network interface

Security Groups



Security Groups



Web Application Firewall (WAF)

- AWS WAF is an HTTP/S deep packet inspection firewall that defends against common web exploits and bots that can affect availability, compromise security, or consume excessive resources
- With AWS WAF, customers can create security rules or use third-party solutions that control bot traffic and block common attack patterns such as SQL injection or cross-site scripting (XSS)
- WAF is usually bundled with Shield Standard for AWS customers

WAF Matching Attributes

- IP addresses of originating requests
- Country that requests originate from
- Values in request headers
  (e.g., User-Agent, Content-Type)
- Literal or regex string patterns that appear in requests (e.g. [cC][mM][dD].[eE][xX][eE])
- Length of requests (buffer overflows)
- Presence of SQL injection code that is likely to be malicious
- Presence of a malicious cross-site scripting attack

Web Application Firewall (WAF)

AWS WAF
Protect your web applications from common web exploits

Create a policy
Build your own rules using the visual rule builder or JSON code, or deploy managed rules maintained by AWS or AWS Marketplace sellers

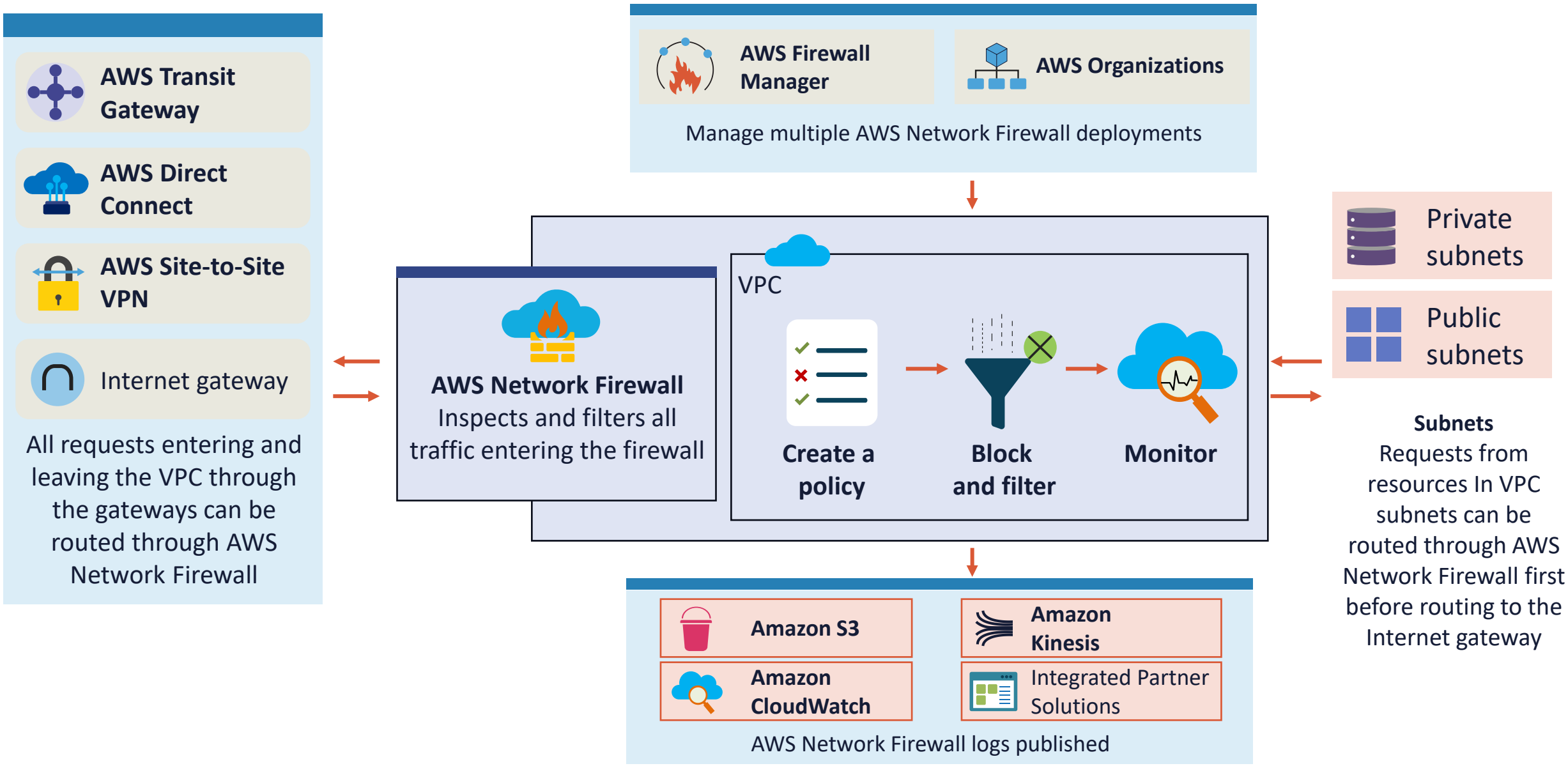
Block and filter
Protect against vulnerabilities and exploits such as SQLi or XSS attacks, and filter out unwanted traffic by IP address or by defining specific patterns

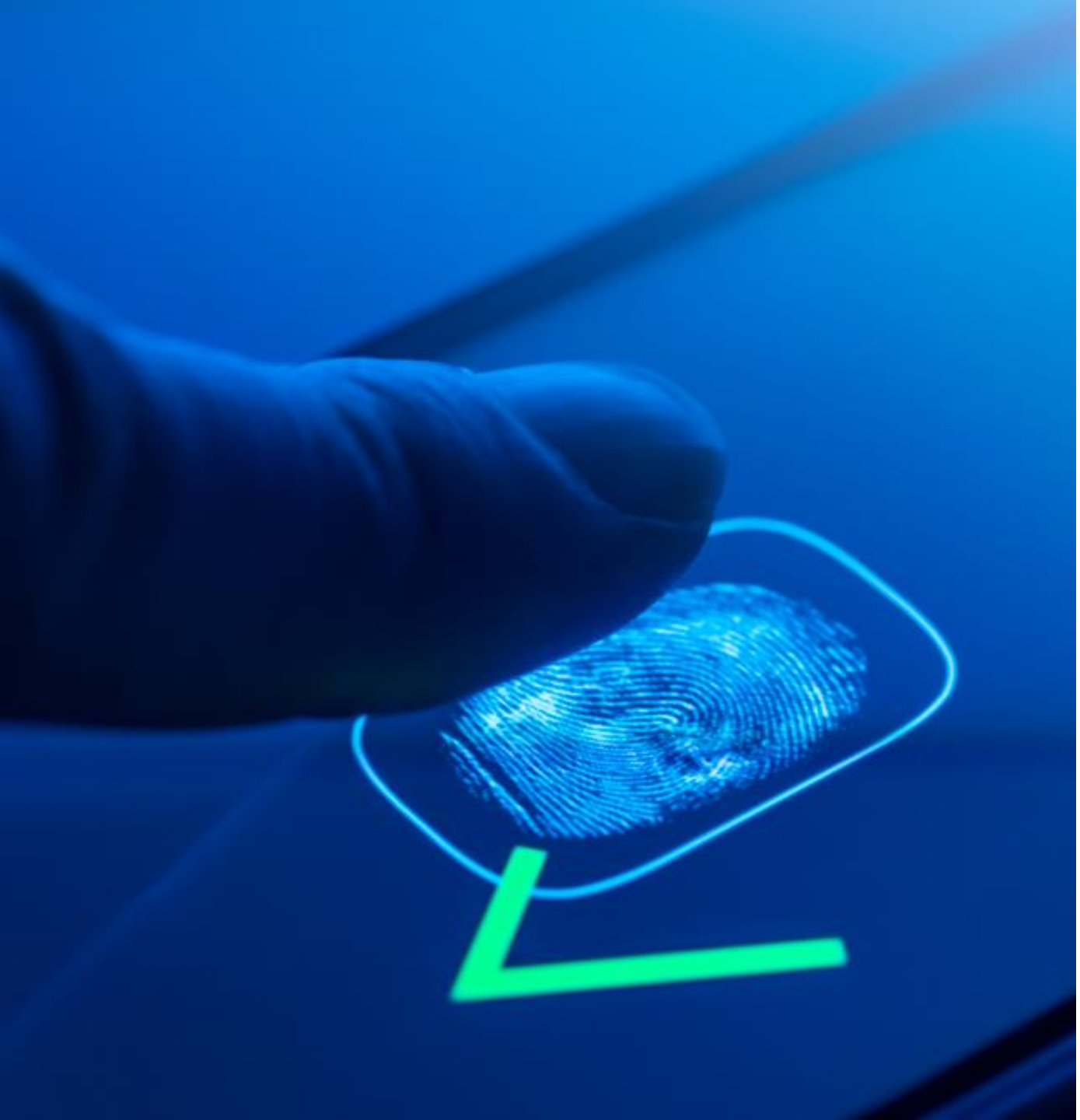
Monitor
Use Amazon CloudWatch to receive incoming traffic metrics and use Amazon Kinesis Data Firehose to request details and tune rules based on metrics and log data

AWS Firewall Manager

- Firewall Manager is an Amazon Web Services security management service that enables clients to centrally configure and administer firewall rules across accounts and applications in AWS Organizations
- As new applications are built or bought, Firewall Manager simplifies the process of introducing them and associated resources into compliance by enforcing a common set of security rules

AWS Firewall Manager





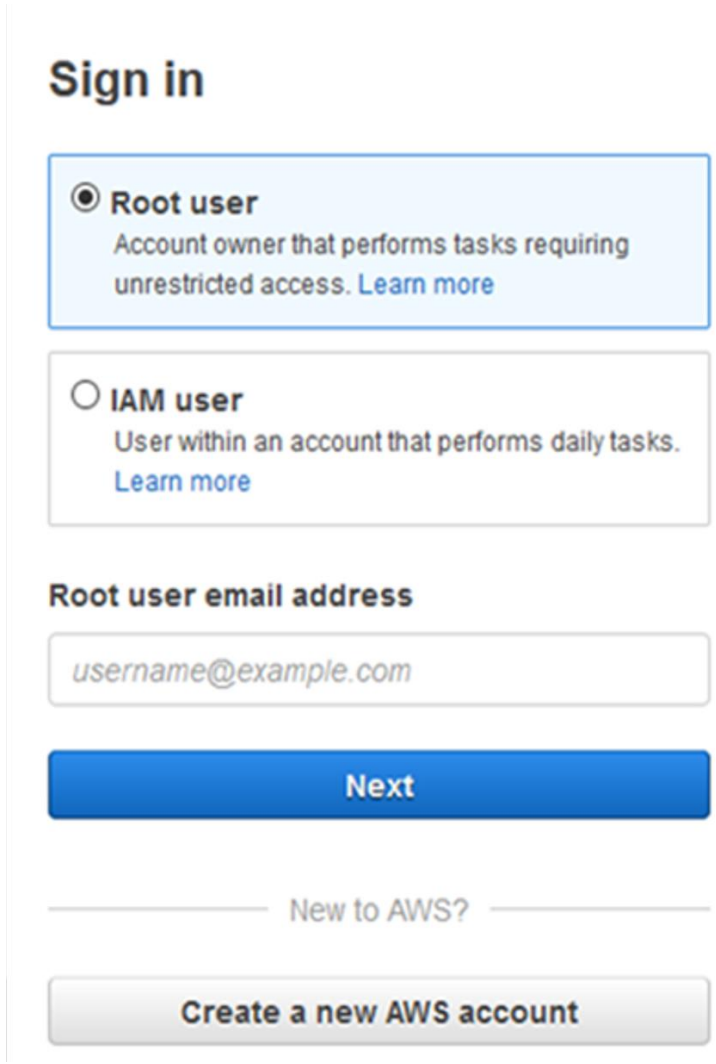
Least Privilege Principle

- Least privilege is the principle that a security architecture should be utilizing so that each subject is granted the minimum system resources and authorizations that the entity needs to conduct its activities
- When related to data and information, this is often called the "need to know" principle
- At AWS, this often applied with a role-based access control (RBAC) model unless federated single sign-on (SSO) is being used

AWS IAM Least Privilege

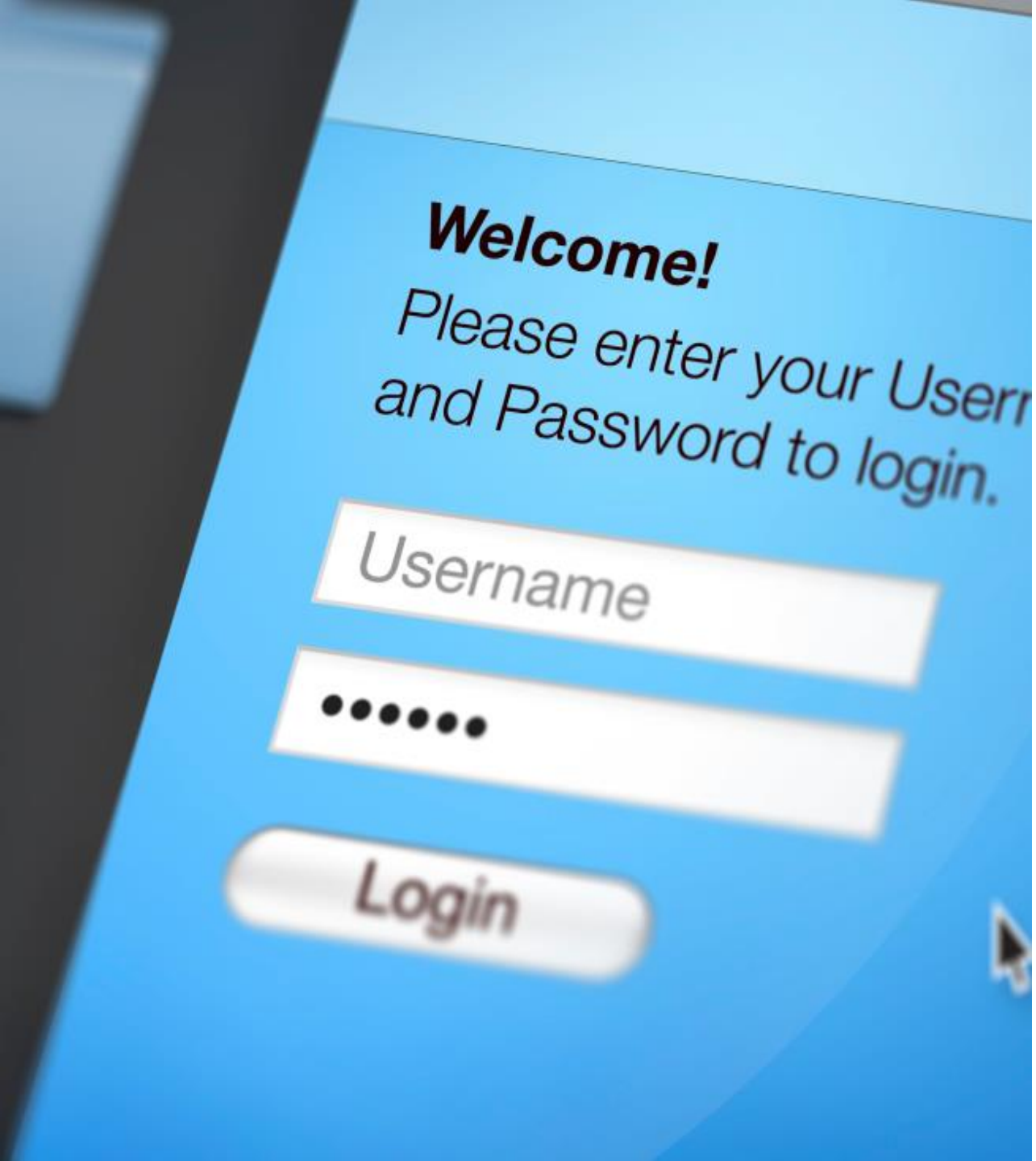
- When setting permissions with Identity and Access Management policies, grant only the permissions necessary to perform a task
- This is accomplished by defining the actions that can be taken on specific resource objects under certain conditions
- Administrators often begin with broader permissions, then subsequently explore the permissions that are needed for a particular workload or use case

Root Account Protection



The AWS Root Account

- When the customer first creates an AWS account, they begin with a single sign-in identity that has complete access to all AWS services and resources in the account
- This identity is called the AWS account root user and is accessed by signing in with the email address and password used to create the account
- The IAM password policy does not apply to the root account
- Always use a physical or software-based multi-factor token access on the root account



Root Account Distinctives

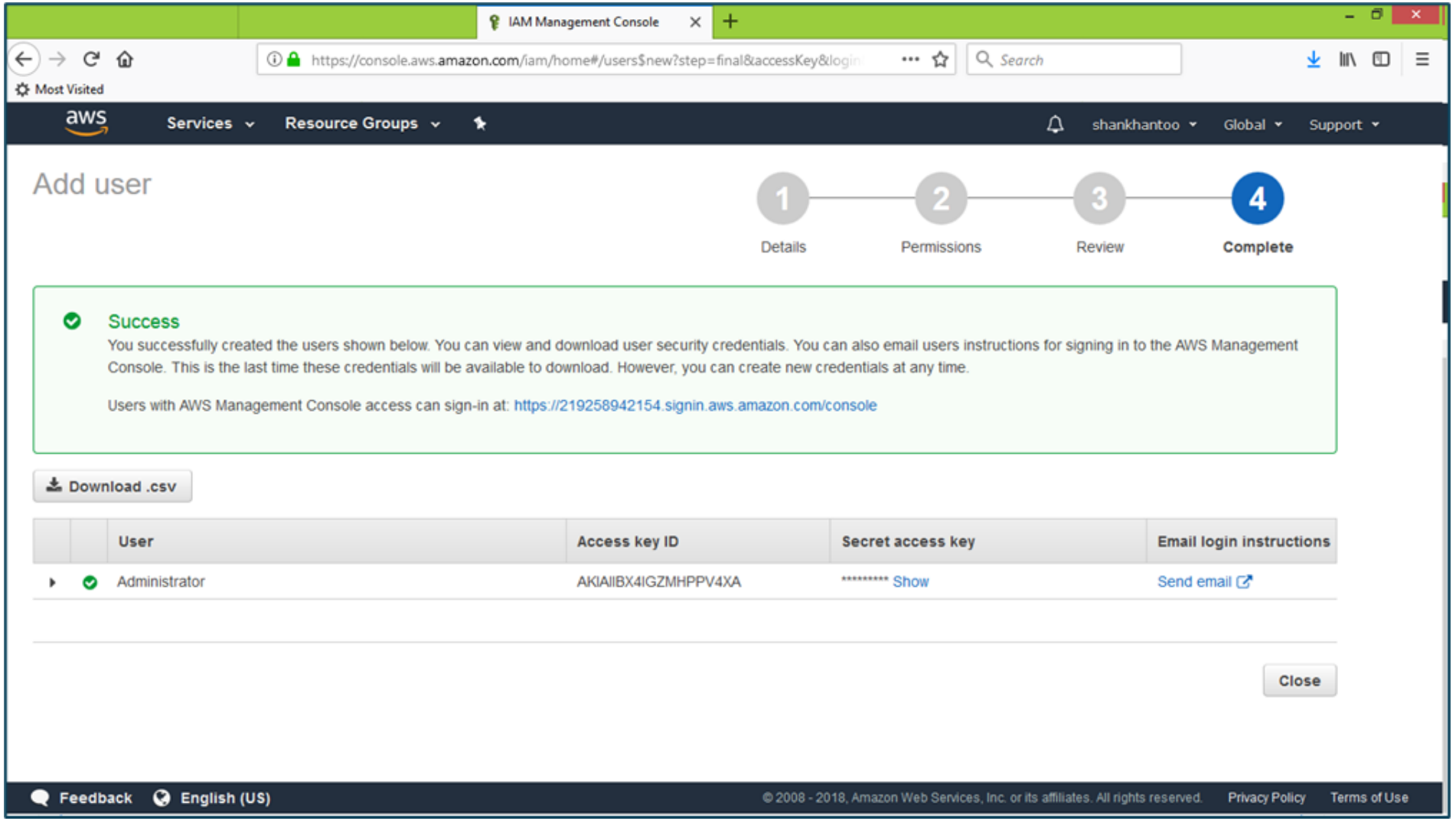
- Customers are strongly discouraged from using the root user for programmatic or everyday tasks
- Root user credentials are only used to perform a few account and service management tasks
- Only the root account user can
  - Change the support plan and modify payment options and billing
  - Close an AWS account
  - Sign up for GovCloud
  - Transfer a Route 53 domain to another account
  - Create an organization

Comparing Multi-Factor Authentication Options

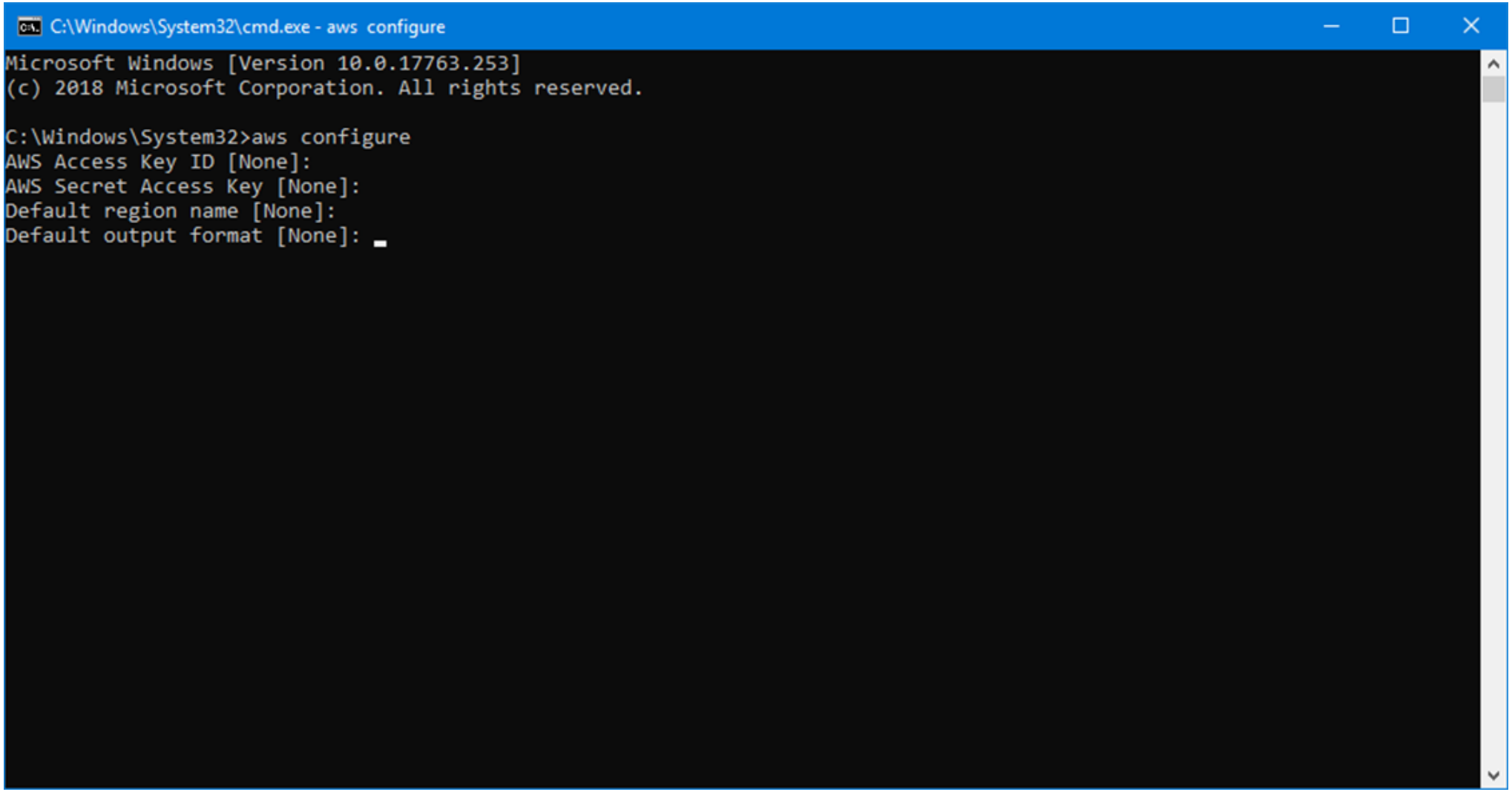
In this demo…

Compare AWS multi-factor authentication options at https://aws.amazon.com/iam/features/mfa/

Programmatic Access to AWS



Programmatic Access to AWS

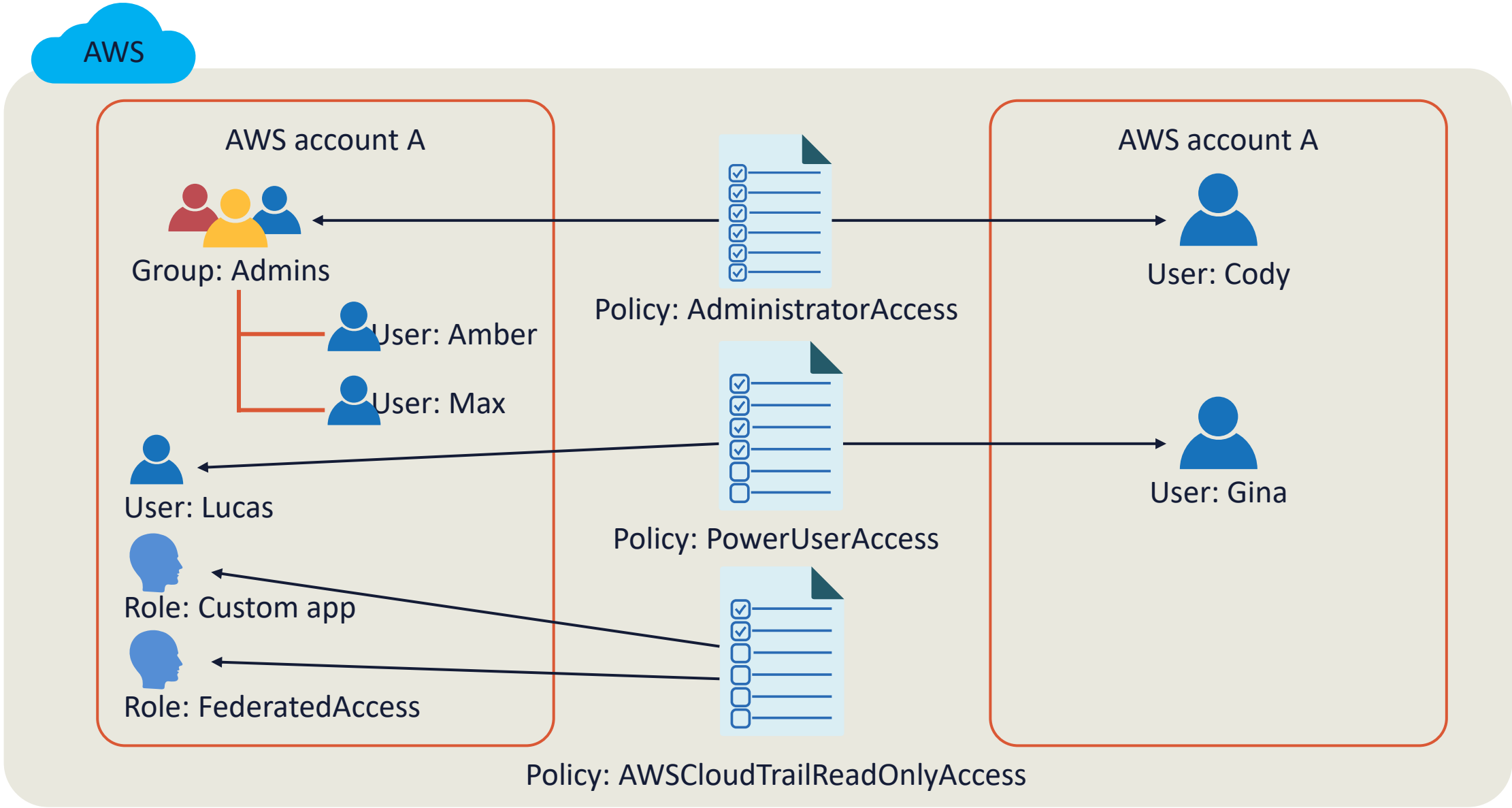


Working With the AWS IAM Service

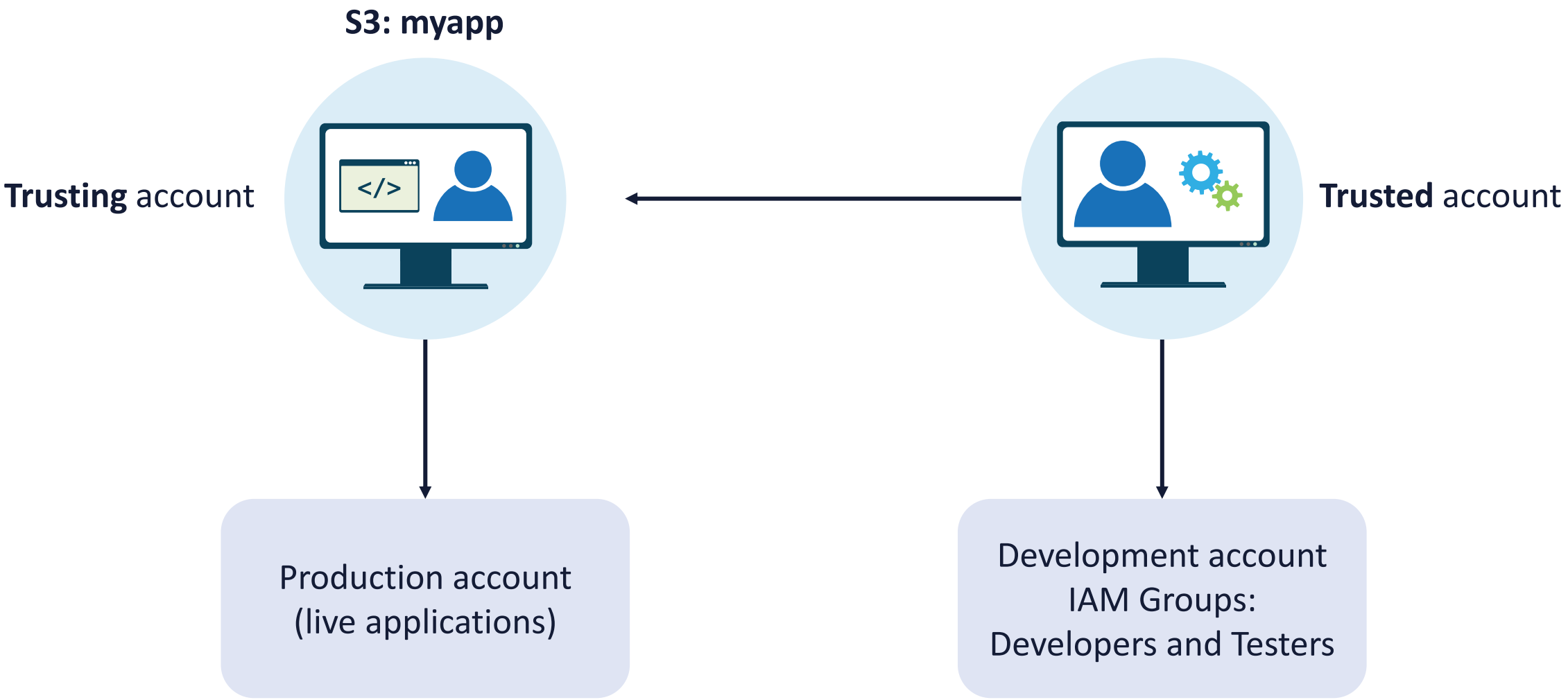
In this demo…

Work with the AWS IAM managed service, password policies, and Identity Center

Roles and Managed Policies



Cross-Account Roles



Systems Manager

- AWS Systems Manager helps you centrally view, manage, and operate nodes at scale across AWS, on-premises, and multicloud environments
- It consolidates various tools into a unified console, enabling automation, troubleshooting, and secure remote management without requiring direct server access
- Systems Manager provides visibility into your infrastructure, allowing you to monitor and manage resources efficiently while ensuring compliance and security
- Additionally, it offers automation capabilities to streamline operational tasks, such as patch management, configuration updates, and software installations

AWS Secrets Manager

- AWS Secrets Manager is a service that helps you securely store, manage, and retrieve sensitive information like database credentials, API keys, and other secrets
- It eliminates the need for hard-coded secrets in application source code by allowing dynamic retrieval at runtime
- Secrets Manager also enables automatic rotation of secrets, reducing the risk of long-term exposure and enhancing security
- Additionally, it integrates with AWS IAM to control access and supports monitoring through AWS CloudTrail and Amazon CloudWatch

Amazon Cognito