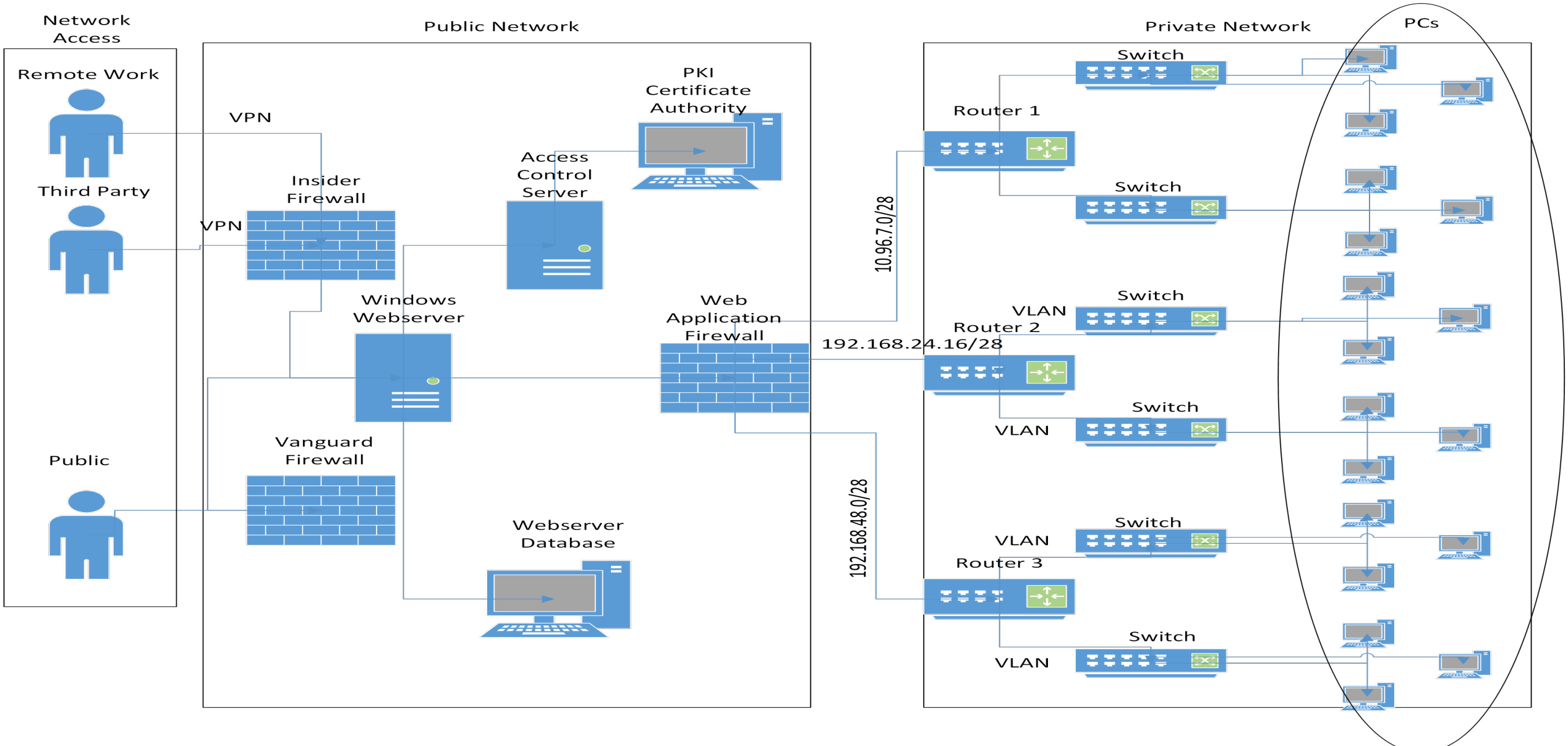
Pre-Migration Presentation

Secure Data Migration Group 2

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Melissa Genovese

Contents

Where We Are:
On Premise Topology



Routers and Switches that lock down:
- Unauthorized domains
- Unauthorized IP Ranges
- Unauthorized port ranges

VPNs for:
- Third parties
- Remote Work

Firewalls that:
- Lockdown unauthorized applications
- Filter public traffic
- Employ VPN

Private network employs:
- DHPC
- VLANS

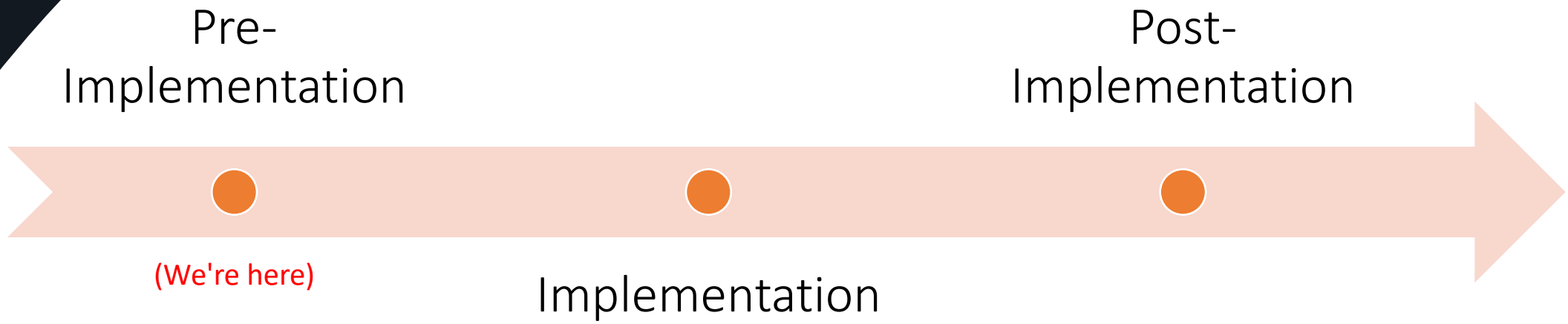
Outside access to server via DNS

Certificate Authority Server

Separate PKI database

Desktops segmented due to different uses

Timeline



What's next?

From on Premises...

To the Cloud

EC2 Compute Container

• EC2 is an Amazon Web Service that is used to create and run virtual machines in the cloud which are called instances.

• Provides scalable computing capacity in the AWS cloud.

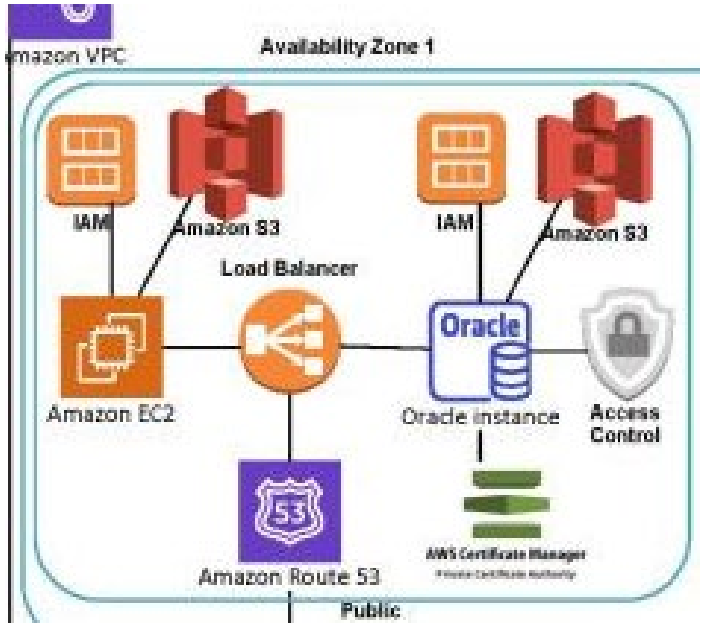
• Can be used to launch as many or as few virtual servers as you need as well as configure security, networking, and manage storage.

Features:

- Preconfigure templates for your instances

- Different configurations for CPU, memory, storage, and network capacity

- Firewall that allows you to specify protocols, ports, and source IP ranges



Amazon S3

•Storage service which offers scalability, data availability, security, and performance.

•Provides management features for optimization, organization and configuring access to data

- Features:

S3 Lifecycle- Configures a lifecycle policy to store objects cost effectively through their lifecycle

S3 Object Lock- Prevents objects from being deleted or overwritten for a fixed amount of time

S3 Replication- Replicates objects, metadata, and tags to different AWS Regions

S3 Batch Operations- Manage billions of objects with the S3 console. Can copy, Invoke Lambda function, and restore on billions of objects

AWS Certificate Manager

What is it?

Uses

Service that uses public and private SSL/TSL X.509, which provides the website with a secure connection, to aggregate and manage these certificates. Automates the renewal and purchasing process, eliminating manual updates.

Availability Zones

Provide Resilience

Contributes to disaster recovery plan and continuity by utilizing AWS Regions. These can be isolated providing network segmentation for higher level classified data. Increases scalability, fault tolerance and availability.

Deployment

Methods

- Elastic Load Balancing
- Amazon CloudFront
- Amazon API Gateway
- Integrated Amazon Services

Best Practices

Maintain Customer Trust

- **AWS Cloud formation** – allows you to create quick templates in a test environment
- **Domain validation –** Domain is verified before Amazon's CA issues certificate
- **Adding/Deleting Domain Names –** must go through domain validation process again
- **AWS CloudTrail –** provides access to monitor AWS deployments

AWS Identity and Access Management (IAM)

What is it?

Uses

Replaces traditional access control without losing quality of the security. AWS IAM is providing a central cloud solution to manage permissions and user access to your organization.

First Steps

How it works

- After registering with AWS, locate the AWS Management Console
- Default setting is denied access until permissions are set to "Allow"
- Define roles to employees, and assign permissions to positions

Policies

Permission Types

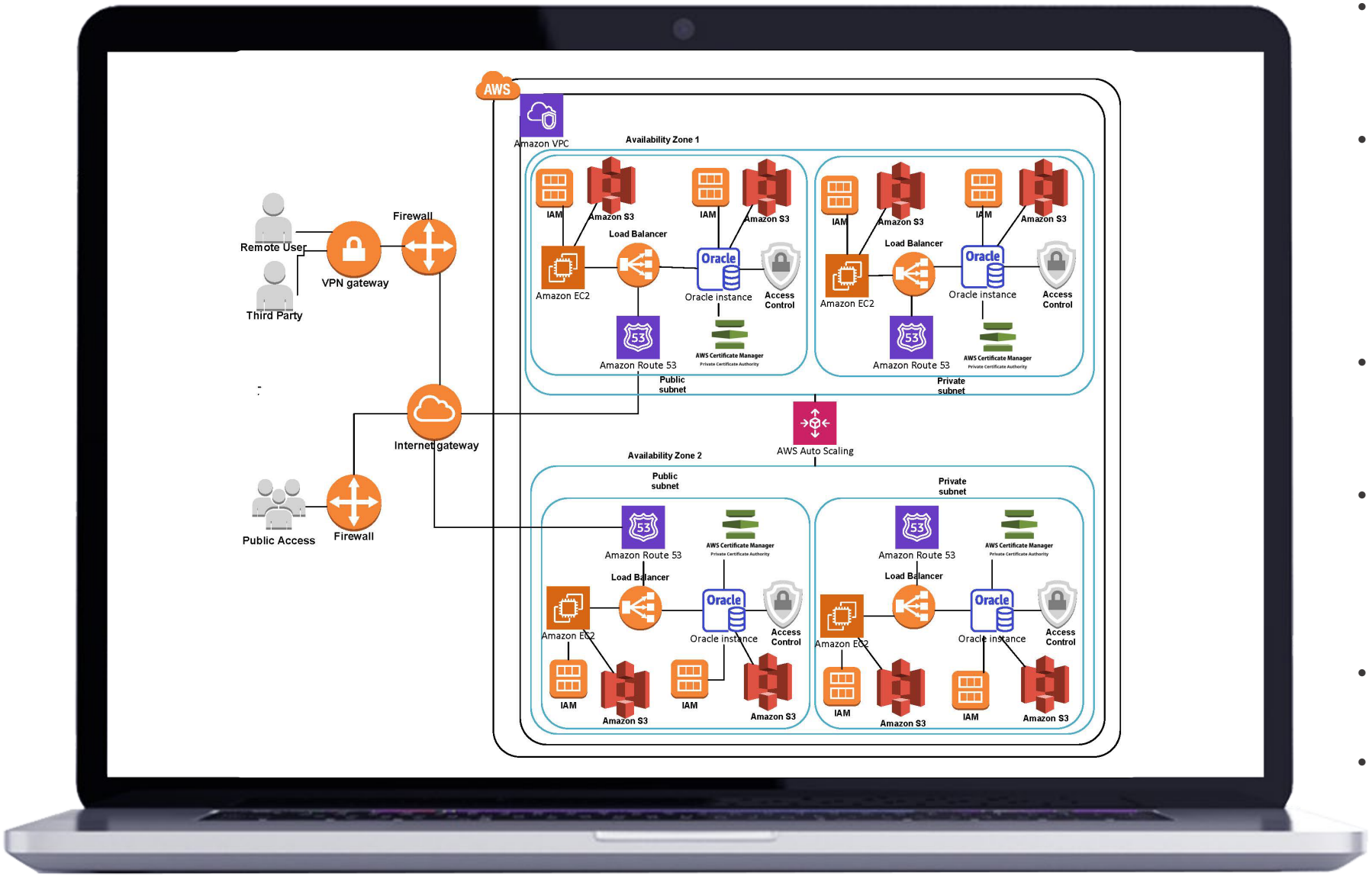
- Identity-Based Policy
- Resource-Based Policy
- Permissions Boundaries
- Organization Service Control Policy (SCP)
- Access Control List (ACL)
- Session Policies

Best Practices

Maintain Security

- Use with multi-factor authentication (MFA)
- Generate least-privilege policies with IAM Access Manager
- IAM policies offers conditions to enforce restricted access
- For long-term employee credential, can rotate access key routinely

AWS Topology



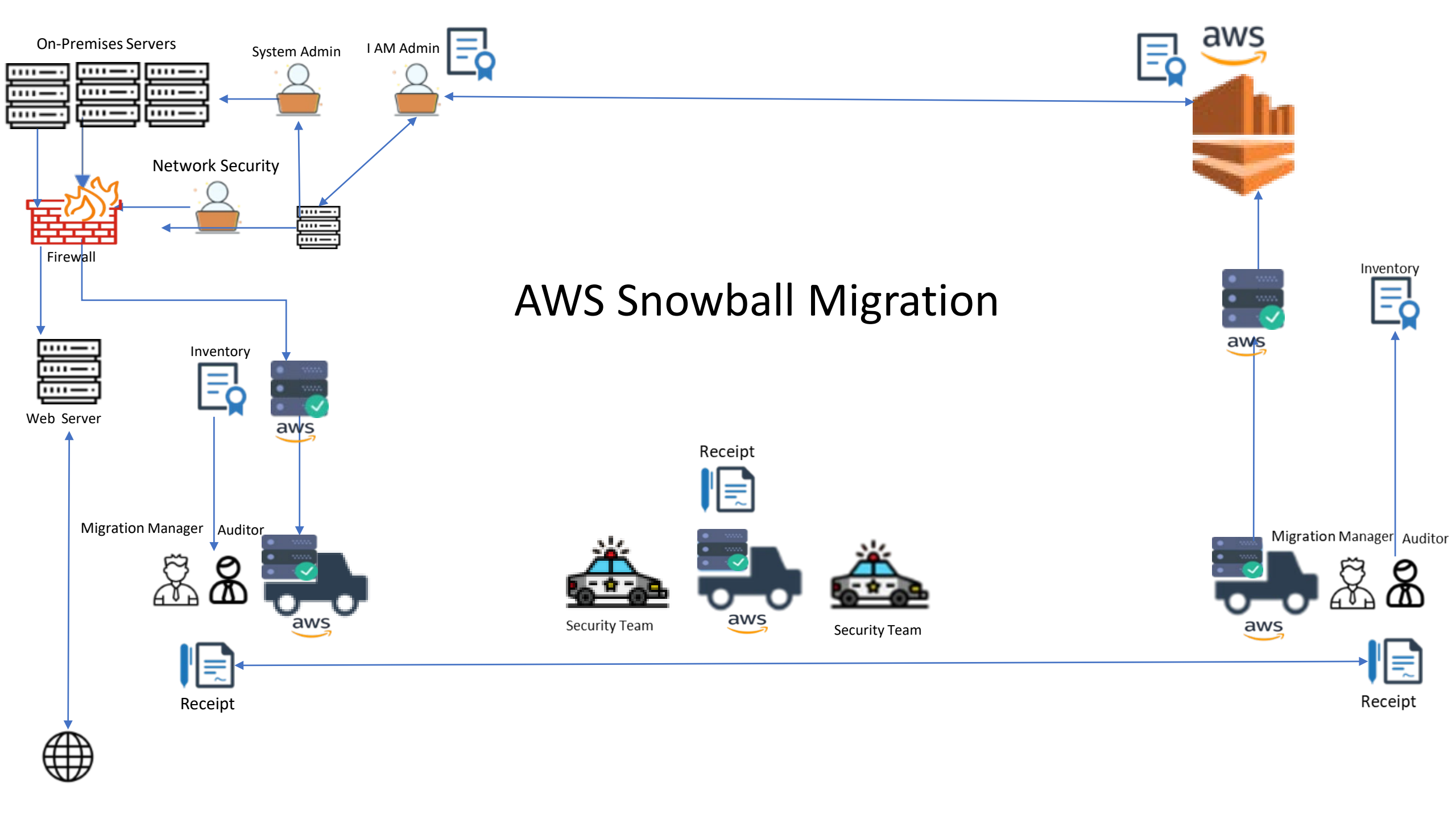
- Amazon VPC gives the company full control over its virtual networking environment.
- The multiple Availability Zones ensure fault tolerance, highly available products, services, and applications, with low latency that is physically separated.
- The Availability zones automatically scale for backing up resources.
- The private subnets secure the company's assets logically by separating them from the public-facing subnet.
- Remote users and third parties can have access to necessary resources.
- The public can access the company website and resources without access to company assets.

Migration from on Premise to AWS Cloud

- Our architecture firm will be utilizing an AWS migration specialist. They will be able to answer any questions and provide support to help our organization with a response time in one business day.

- This will enable our organization to simplify and accelerate migrations, get the support we need, and migrate with confidence knowing everything is secure.

- In this process we will utilize Migration Evaluator, AWS Migration Hub, AWS Application Discover Service, AWS Database Migration Service, Windows on AWS, AWS DataSync, AWS Transfer Family, and AWS Snow Family.



AWS Snowball Migration

References:

AWS Sales Support and Customer Sales Representative Contact Info - Amazon Web Services. (n.d.). Amazon Web Services, Inc. Retrieved September 15, 2022, from https://aws.amazon.com/contact-us/sales-support-migration/?pg=mig-hto&sec=hr&sc_category=category&sc_campaign=wcu&sc_channel=wst&trk=wcu-category

What is AWS Certificate Manager? (2022). Amazon. https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html

IAM. (2003). *Amazon*. Amazon. Retrieved from https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

Post-Migration Presentation

Secure Data Migration Group 2

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Melissa Genovese

Contents

AWS IaaS

In the AWS infrastructure we've implemented our network.

Our Share of Responsibility:

- Systems Configuration
- Updates
- Policy Implementation
- Software maintenance

AWS Share of Responsibilities:

- Physical security
- Availability

Amazon Route 53

With Amazon Route 53 we can:

- Lock down unauthorized domains
- Lock down unauthorized IP Ranges
- Lock down unauthorized port ranges

Amazon Route 53 is a scalable and highly available Domain Name System service with capabilities to:

- Connect user requests to internet applications running on AWS or on-premises.
- Manage network traffic globally

Service Agreements

Customer

AWS Agreement

This agreement holds the terms and conditions that will allow access and usage for AWS' service offerings. Consumer acknowledges lawful entrance to contract, confirms the legality binding consumer to agreement.

Maintaining

Services

Consumer bears the responsibility for upkeep in licenses and staying within license terms. Upgrades, patches and other bug fixes may rollout periodically given AWS has provided prior notice within reason.

Standard

Contractual Clause

Also known as SCC, will be applied when GDPR is involved in usage with AWS services and customer data processing. This includes but is not limited to onward transfers to countries outside the EU.

Outposts

Servers

If run locally on AWS, will have its own set of specific compliance and assurance software in the AWS Outpost scope. This can be circumvented if the consumer lists Outpost separately for the compliance and assurance program.

Third-Party Agreements

Usage

With AWS

AWS allows third-party content to be used at the consumer's discretion. The Third-Party content is controlled by the agreement along with separate terms and conditions and may include additional charges.

Data

Ownership

Any Third-Party data provided to AWS will signify we, the consumer, represent and provide consent for Third-Party data to be shared with AWS and its affiliates for processes and use by AWS.

Transactions

With Third-Parties

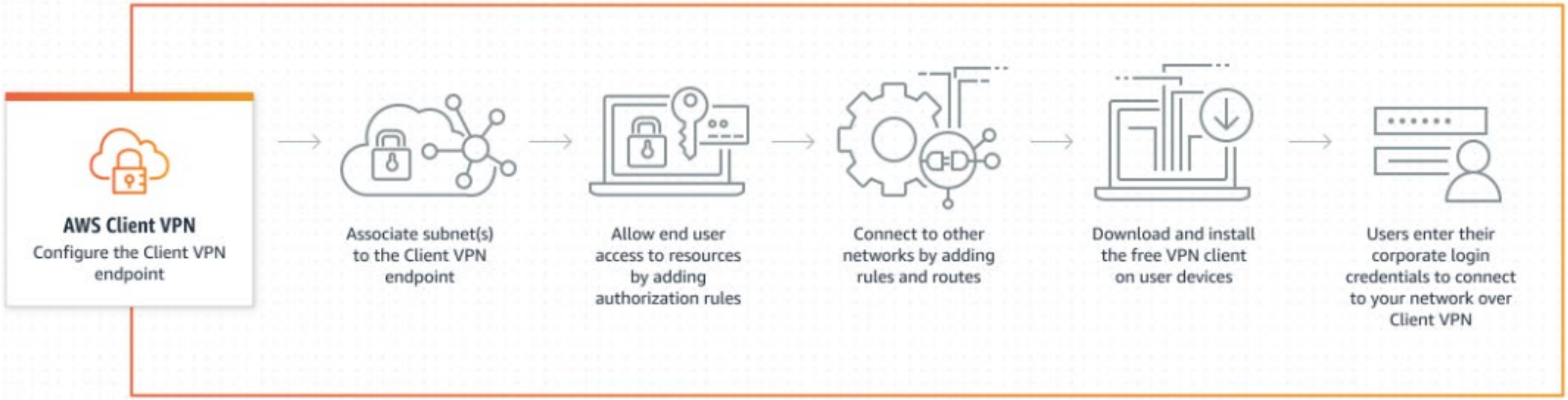
Consumers are given the right to disclose when a third-party is involved in a transaction. That information will then be shared with AWS to allocate with said third-party. Subscriptions may be managed by a third-party agreement through AWS.

Providers

Employed by AWS

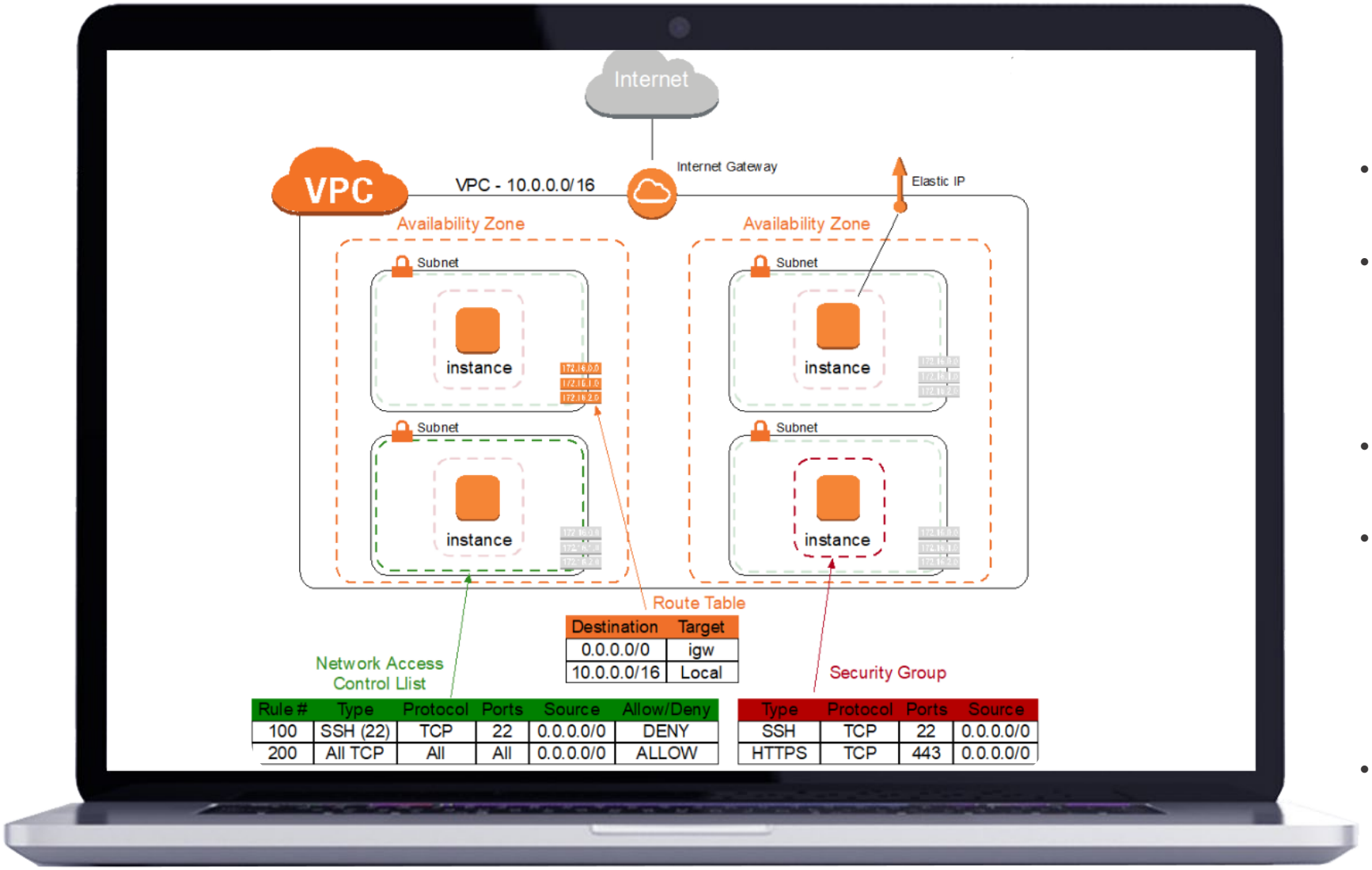
AWS maintains the right to employ external companies to deploy necessary functions under the alias of AWS. Third-party providers will have access to consumer PII only to perform duties in accordance with AWS' privacy notice.

Client VPN



- Remote users or third parties can access from anywhere in the world so long as they have an internet connection.
- Uses a secure TLS connection.
- It scales automatically depending on the number of users are connecting to the organizations AWS resources.
- Customizable security controls defined by network-based access rules via Active Directory or Security Groups.
- Client authentication using federated authentication, certificate-based authentication, and Active Directy.
- Can view connection logs which includes connection attempts, and you can terminate current connections.

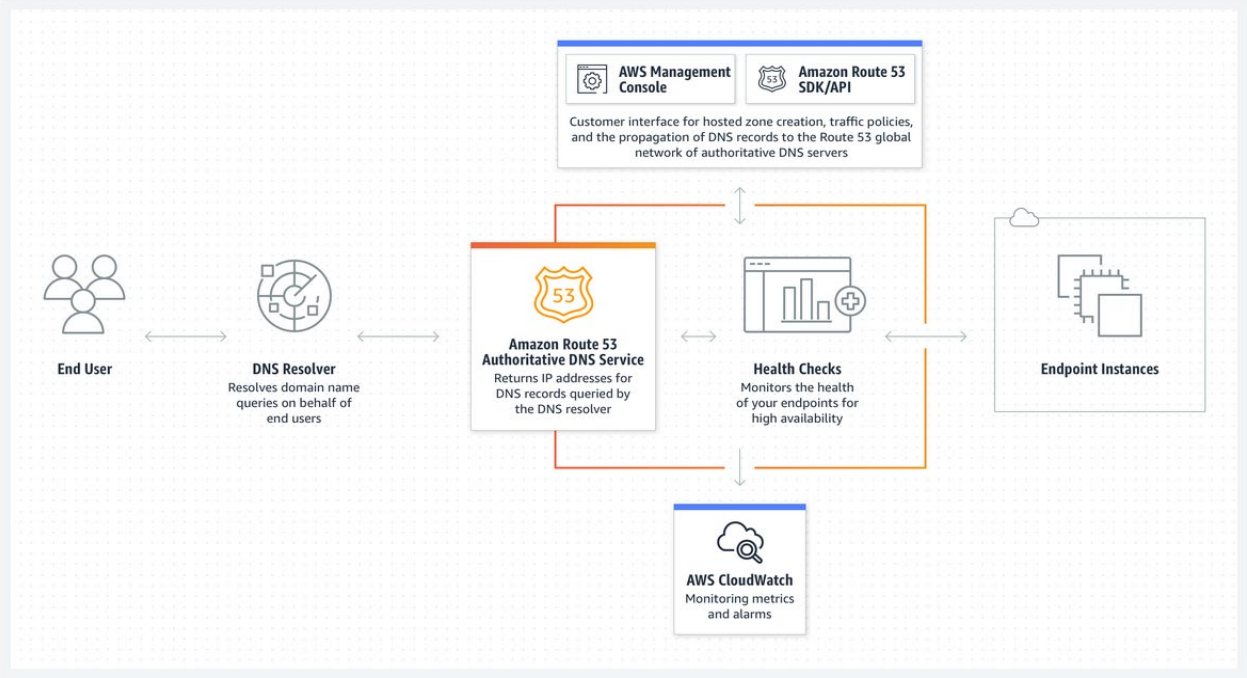
AWS SUBNETS



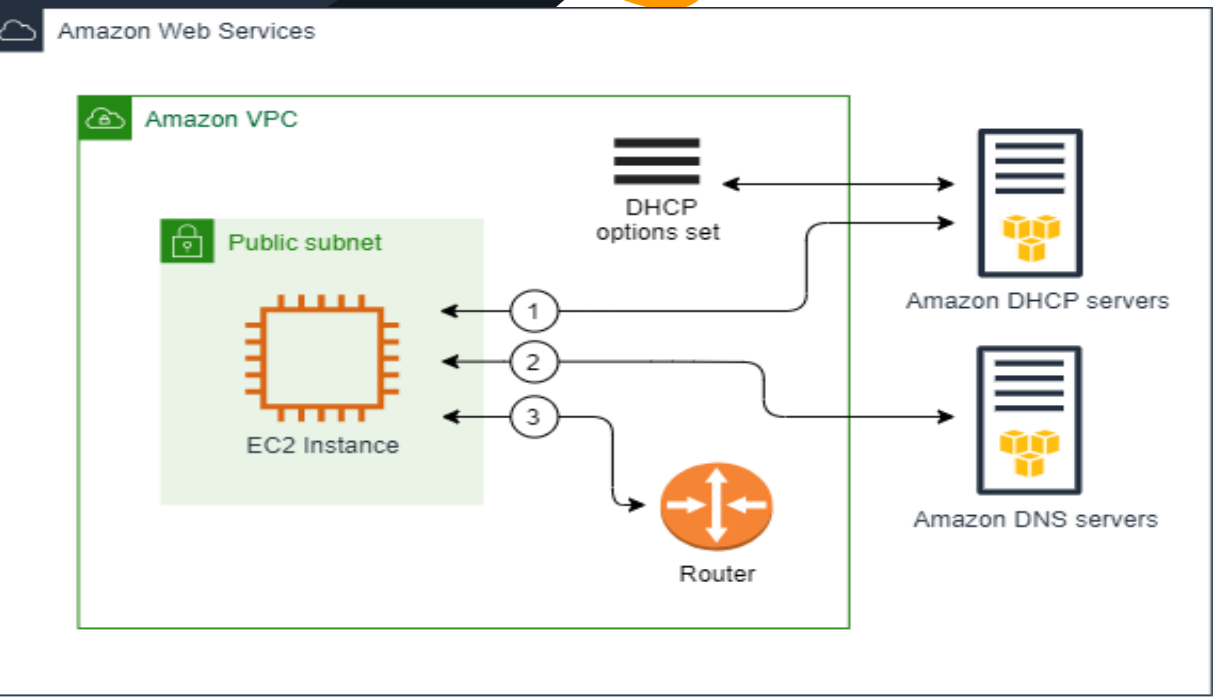
- Amazon VPC is an isolated section on the AWS infrastructure where an organization's resources can be placed.
- Subnets can be created in the Amazon VPC, Public and Private.
- Private subnets secure the company's assets logically by separating them from the public-facing subnets.
- Subnets can be used to manage resources in the organization.
- Security Groups control inbound and outbound traffic for the EC2 instances and network ACLs control inbound and outbound traffic for the subnets.
- Our organizations two Windows and two Linux EC2 instances each have their own subnet for easy management.

Domain Name System (DNS)

- Amazon Route 53 is a highly available and scalable Domain Name System (DNS) web service
- Create, visualize, and scale complex routing relationships between records and policies
- Set routing policies to pre-determine and automate responses in case of failure
- Assign and access custom domain names in your Virtual Private Cloud (VPC)



DHCP



- Gives you control of the DNS servers, domain names, or NTP servers used by the devices in your Virtual Private Cloud
- Can disable DNS resolution in your VPC
- Applications running on EC2 instances in subnets can communicate with Amazon DHCP servers as needed to retrieve their IP address lease
- Can specify the network configurations that are provided by Amazon DHCP servers by using DHCP option sets

Amazon Time Sync Services

What is Amazon Time Sync Services?

- It is an Amazon's time synchronization service delivered over NTP.
- It was launched in November 2017 to help instances maintain accurate time.
- It is a natively accessible from Amazon EC2 instances and this can be pushed to edge devices.
- Uses a fleet of redundant satellite-connected and atomic clocks in each Region to deliver a highly accurate reference clock.

What are its benefits?

- It help instances maintain a more accurate time.
- The service is provided at no additional charge.
- It is available to all EC2 instances in all AWS Regions and AWS GovCloud (US) Region.

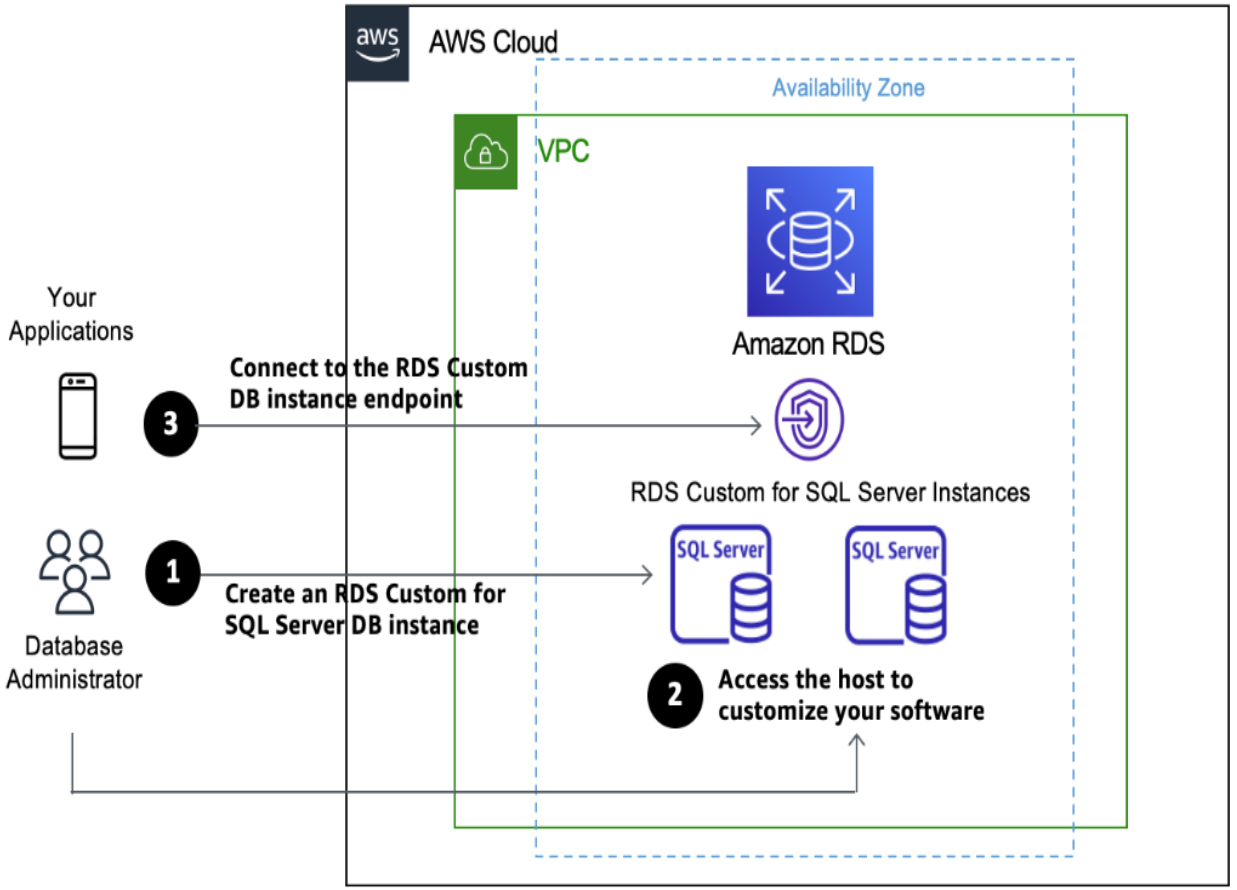
Amazon RDS Custom for SQL DB

What is Amazon RDS Custom for SQL DB?

- RDS Custom for SQL Server, can enable features that require elevated privileges like SQL Common Language Runtime (CLR), install specific drivers to enable heterogenous linked servers, or have more than 100 databases per instance.

Use Cases:

- Run legacy, custom, and packaged business applications
- Build web and mobile applications
- Develop ecommerce applications



Amazon Certificate Manager Service

What is AWS Certificate Manager?

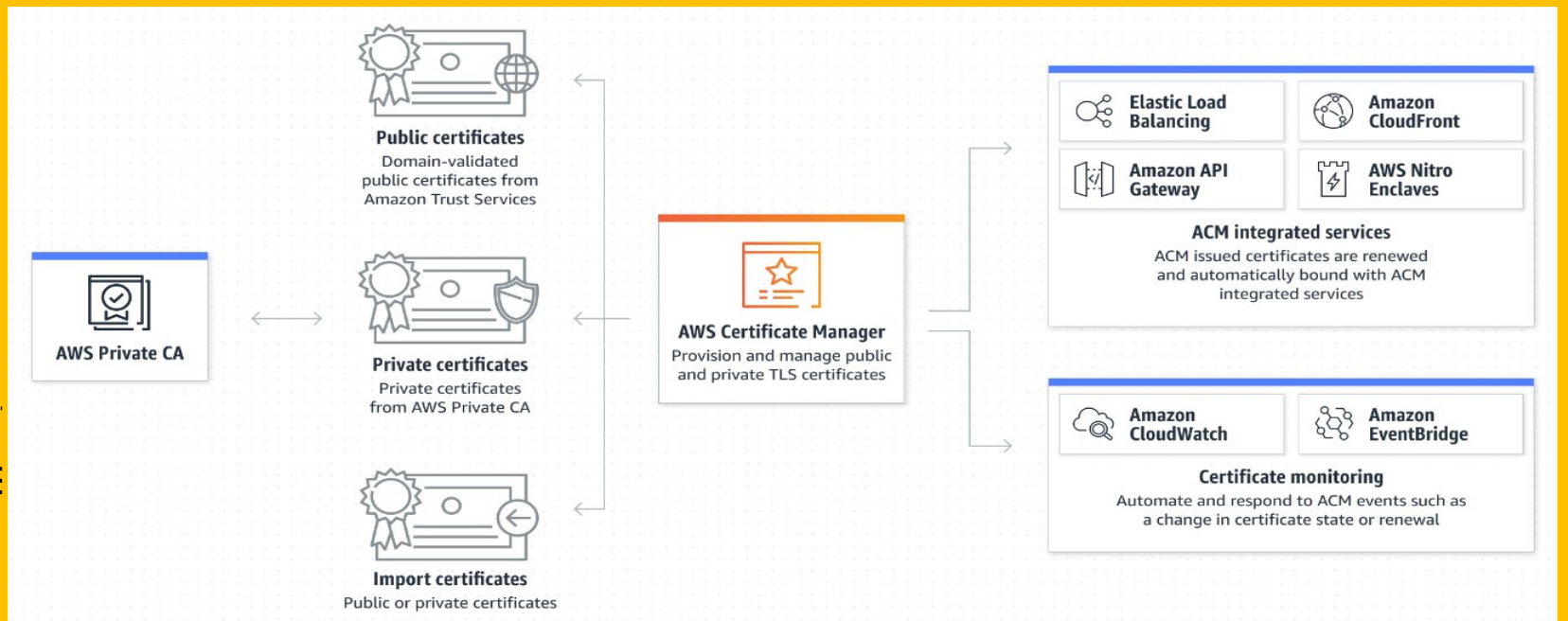
Use AWS Certificate Manager (ACM) to provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and your internal connected resources. ACM removes the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates.

Features:

- Centrally manage certificates
- Secure key management
- AWS service integration
- Import third-party certificates

Use Cases:

- Protect and secure your websi
- Protect your internal resources
- Improve uptime



References:

Amazon Route 53 | DNS service | AWS. (n.d.). Retrieved November 27, 2022, from https://aws.amazon.com/route53/

Amazon Web Services. (2011). *AWS Certificate Manager Features*. Amazon. Retrieved November 30, 2022, from https://aws.amazon.com/certificate-manager/features/

Amazon Web Services. (n.d.). *AWS VPN*. Amazon. Retrieved November 21, 2022, from https://aws.amazon.com/vpn/

Amazon Web Services. (n.d.). *Subnets for your VPC*. Amazon. Retrieved November 20, 2022, from https://docs.aws.amazon.com/vpc/latest/userguide/configure-subnets.html

Amazon Web Services. (n.d.). *What is AWS Client VPN?* Amazon. Retrieved November 21, 2022, from https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/what-is.html

Channy Yun, https://aws.amazon.com/blogs/aws/new-amazon-rds-custom-for-sql-server-is-generally-available(2021)

Colegio Oficial de Médicos de la Provincia, Valladolid. (2016). *VPC: Validación Periódica de La Colegiación*. Amazon. Retrieved November 27, 2022, from https://docs.aws.amazon.com/vpc/latest/userguide/DHCPOptionSetConcepts.html

Colegio Oficial de Médicos de la Provincia, Valladolid. (2016). *VPC: Validación Periódica de La Colegiación*. Amazon. Retrieved November 27, 2022, from https://docs.aws.amazon.com/vpc/latest/userguide/VPC_DHCP_Options.html

Matthews, N. (2016, March 29). *Amazon VPC for On-Premises Network Engineers – Part 1*. Amazon. Retrieved November 21, 2022, from https://aws.amazon.com/blogs/apn/amazon-vpc-for-on-premises-network-engineers-part-one/

www.docs.aws.amazon.com, https://docs.aws.amazon.com/wellarchitected/latest/iot-lens-checklist/best-practice-12-2.html