AWSOME DAY
ONLINE CONFERENCE

Introduction to AWS services
Networking & security

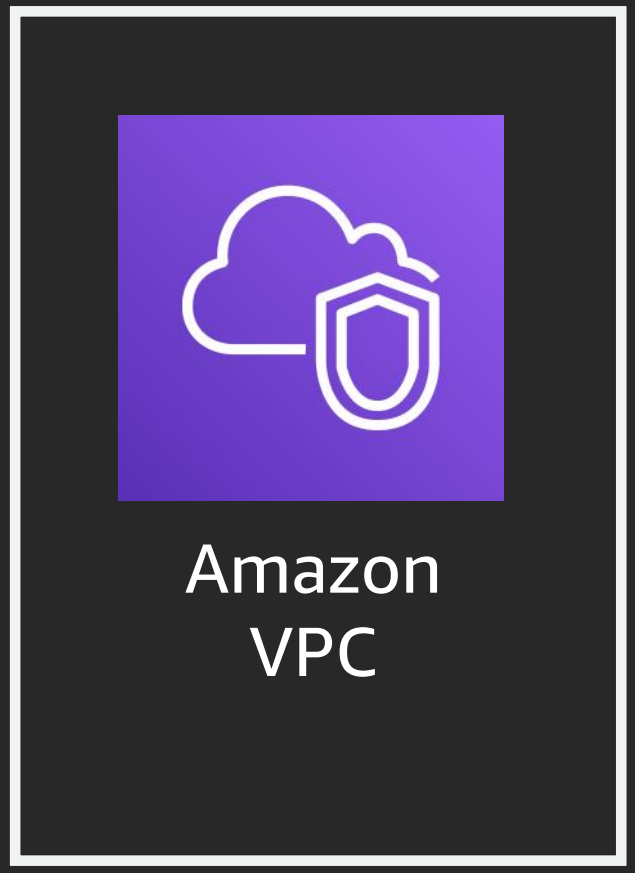
Joel Skepper

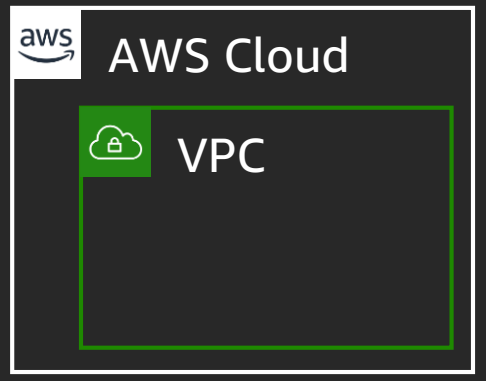
Technical Trainer
Amazon Web Services

aws | intel

Networking

Amazon Virtual Private Cloud (Amazon VPC)





Your private network space in the AWS Cloud

Provides logical isolation for your workloads

Allows custom access controls and security settings for your resources

aws | intel

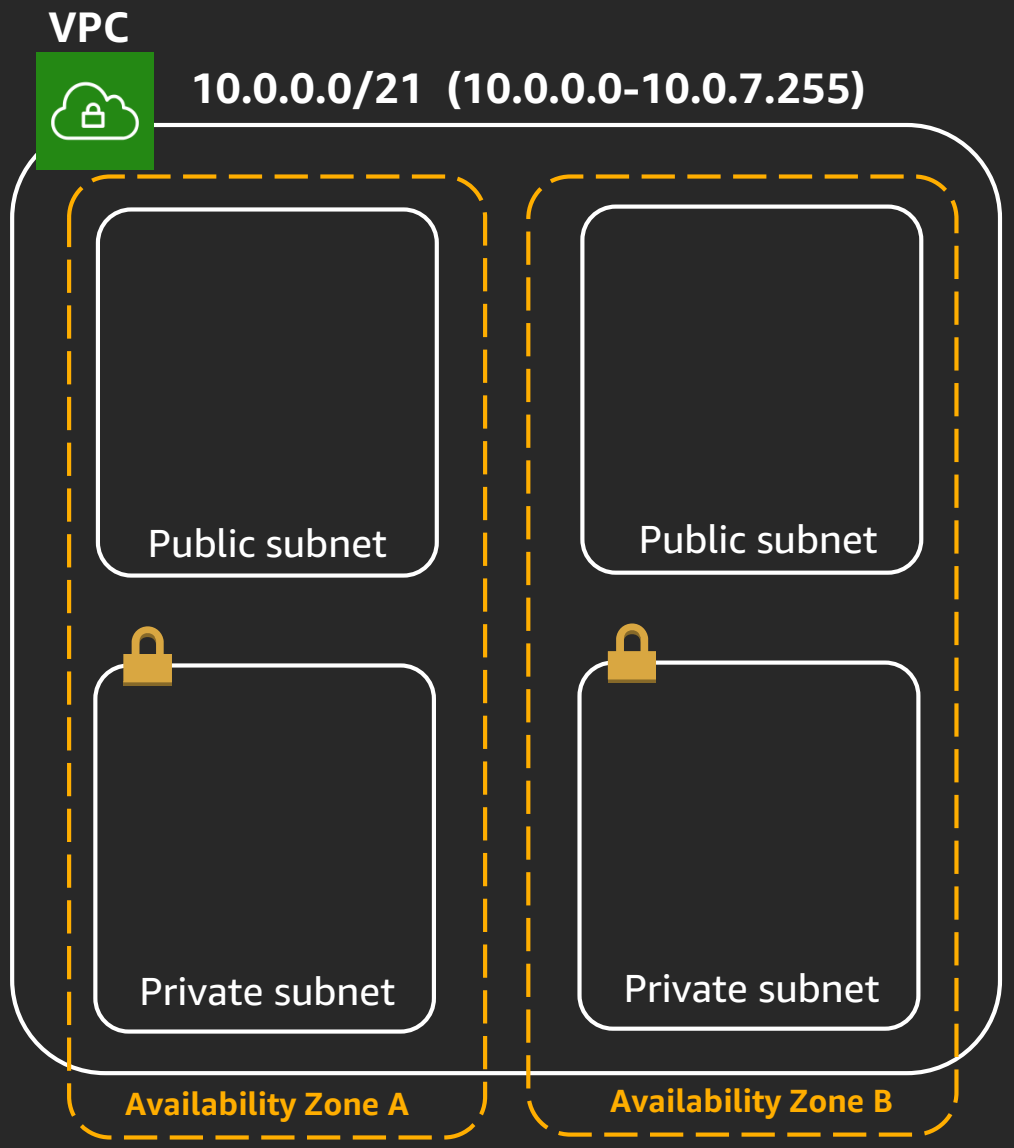
Using subnets to divide your VPC

A subnet is a segment or partition of a VPC's IP address range where you can isolate a group of resources.

Subnets define internet accessibility

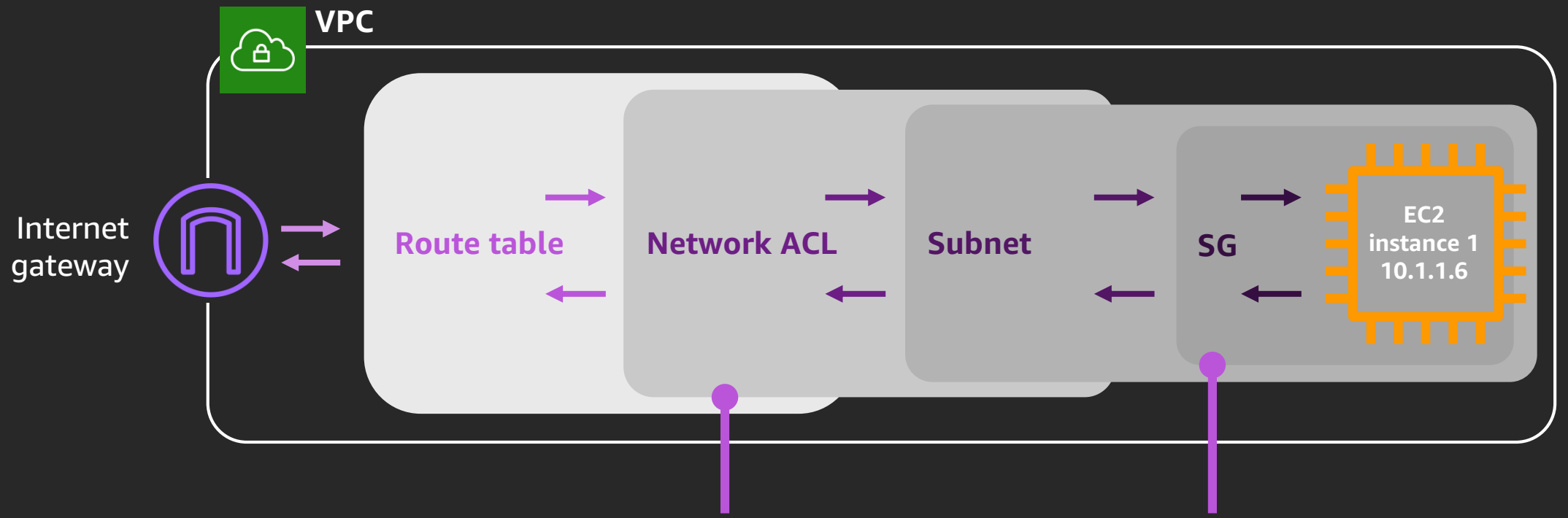
Private subnets

- No routing table entry to an internet gateway
- Not directly accessible from the public internet



aws | intel

Structure your infrastructure

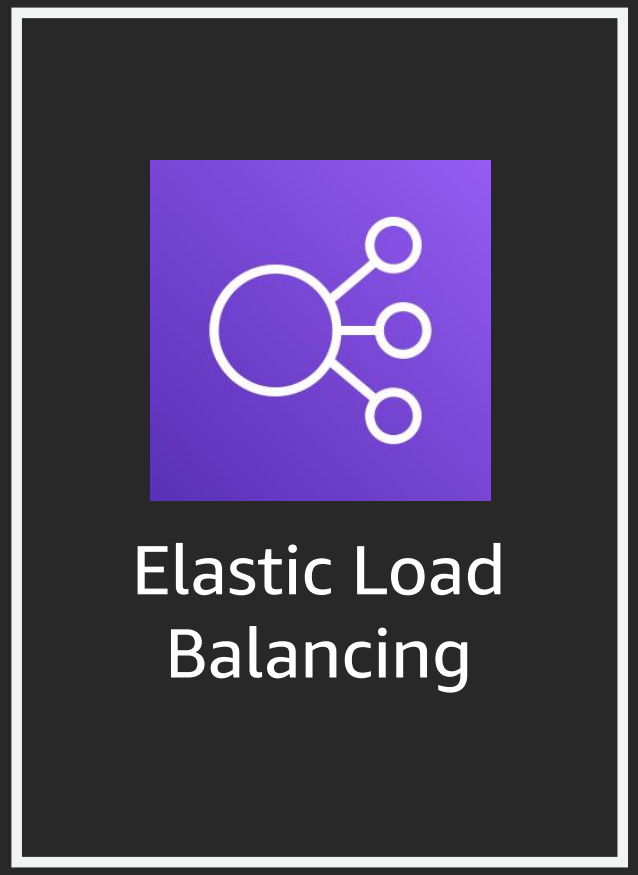


- **Network access control lists (ACLs)**
- Allow/deny traffic in and out of subnets
- Hardens security as a secondary level of defense at the subnet level

Security groups

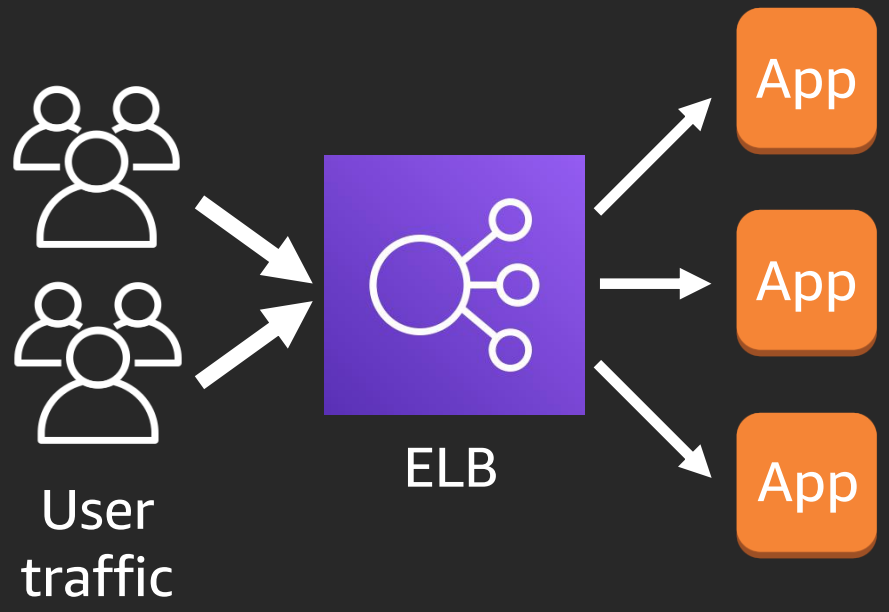
- Used to allow traffic to/from at the network interface (instance) level
- Usually administered by application developers

Elastic Load Balancing (ELB)

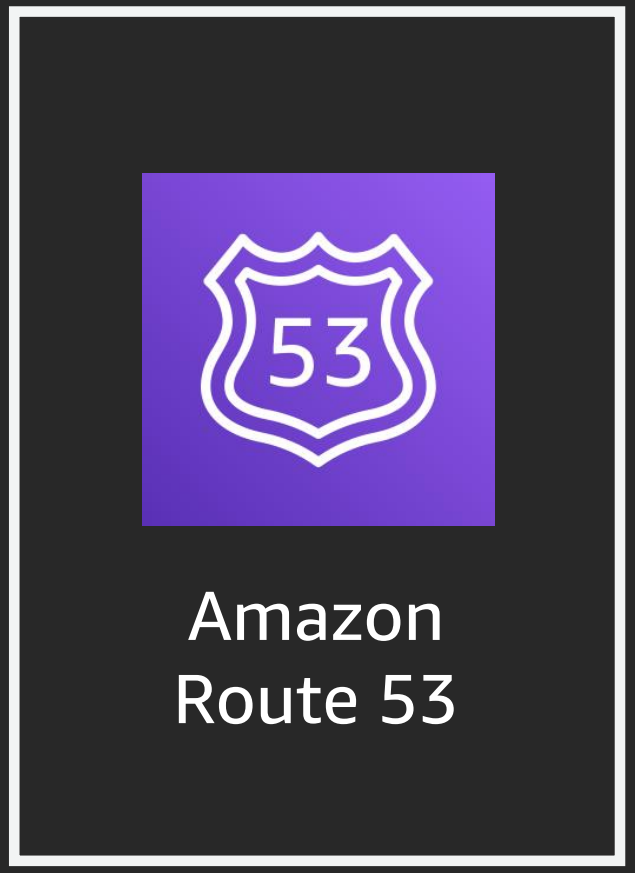


A managed load balancing service that distributes incoming application traffic across multiple Amazon EC2 instances, containers, and IP addresses.

- High availability
- Health checks
- Security features

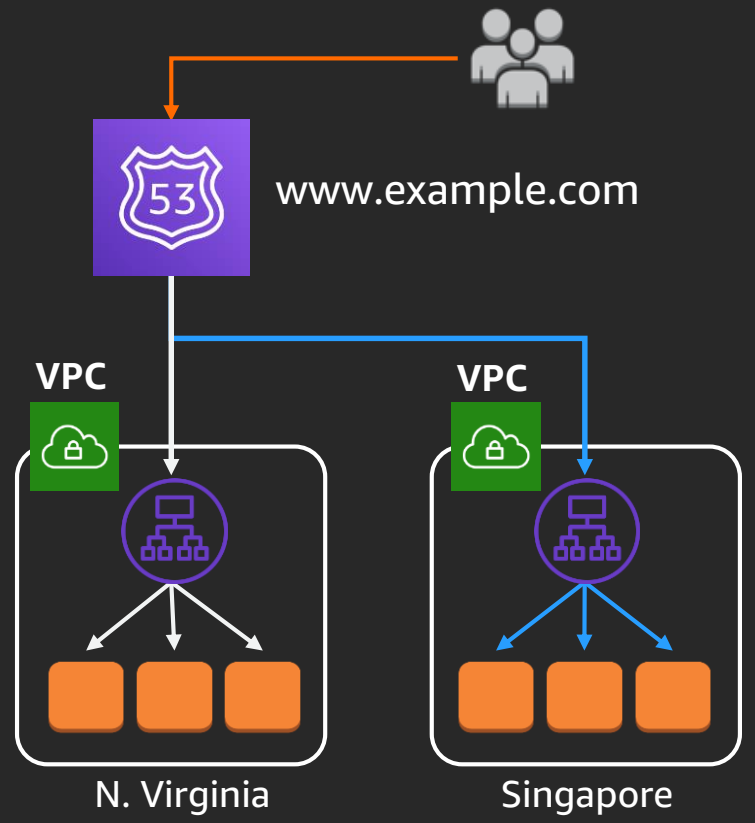


Amazon Route 53



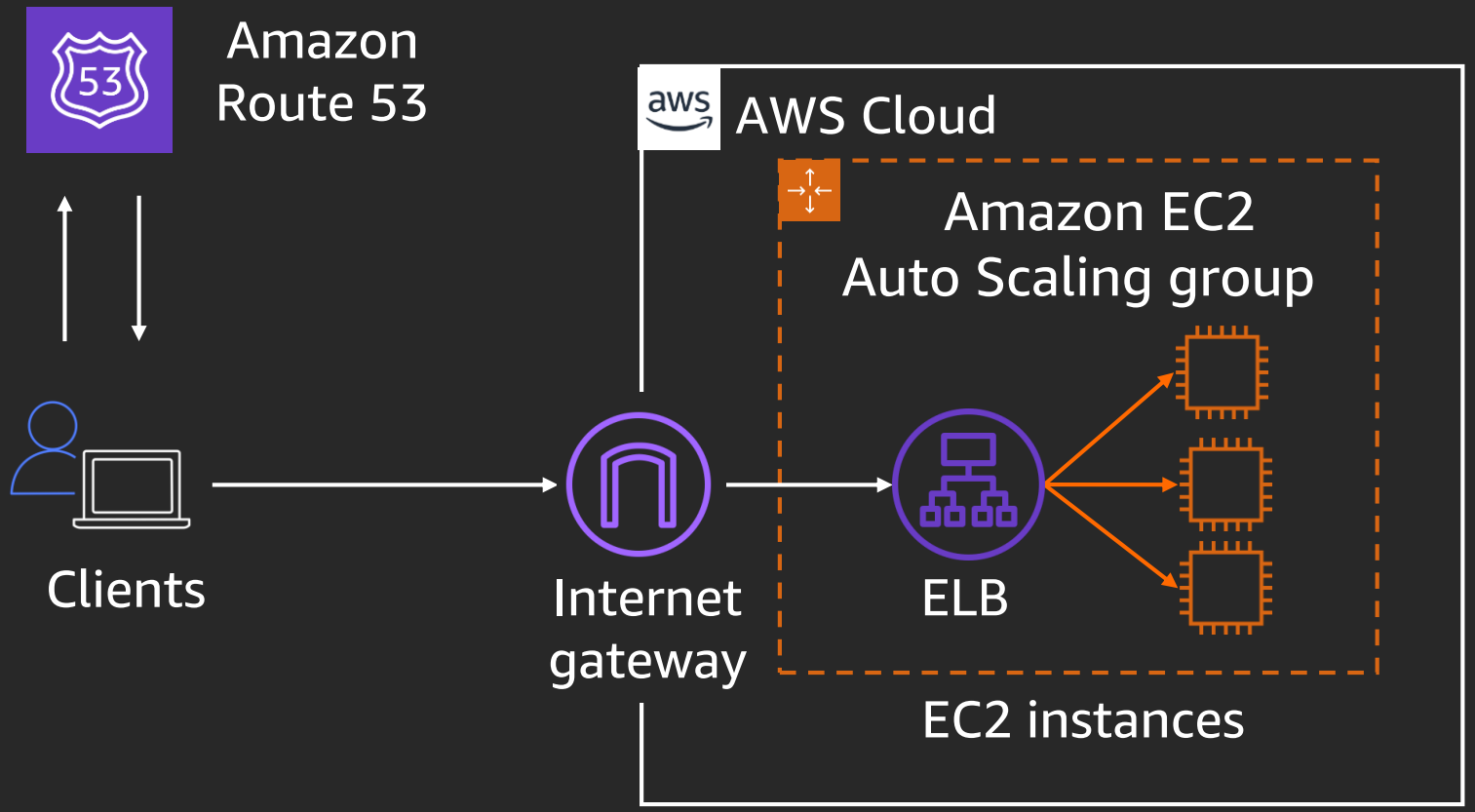
Route 53 is a highly available and scalable cloud Domain Name System (DNS) service

- DNS translates domain names into IP addresses
- Able to purchase and manage domain names and automatically configure DNS settings
- Provides tools for flexible, high-performance, highly available architectures on AWS
- Multiple routing options



aws | intel

Putting it all together



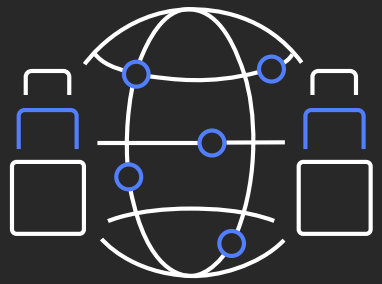
Security

Security is our top priority

Designed for security

Constantly monitored

Highly automated

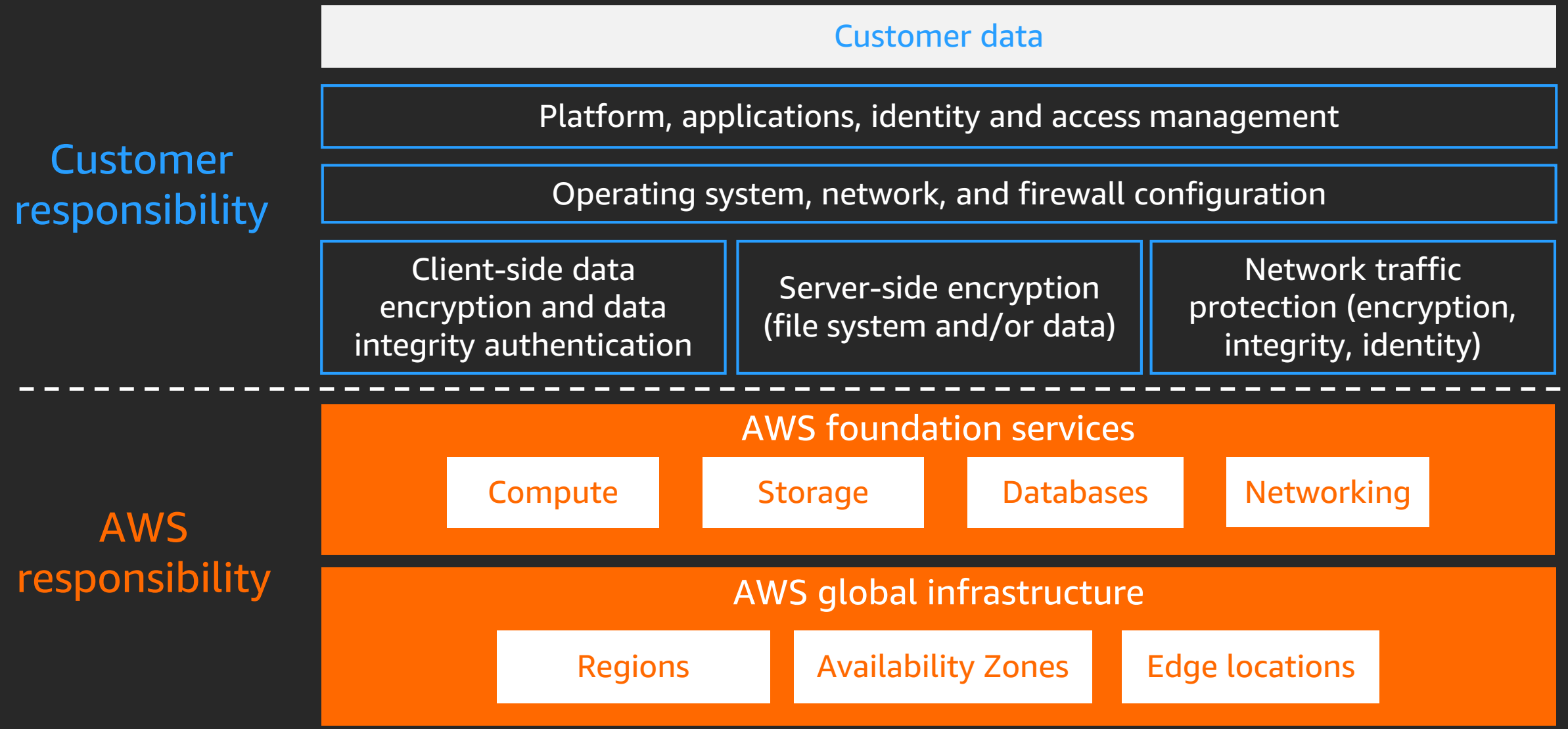


Highly available

Highly accredited

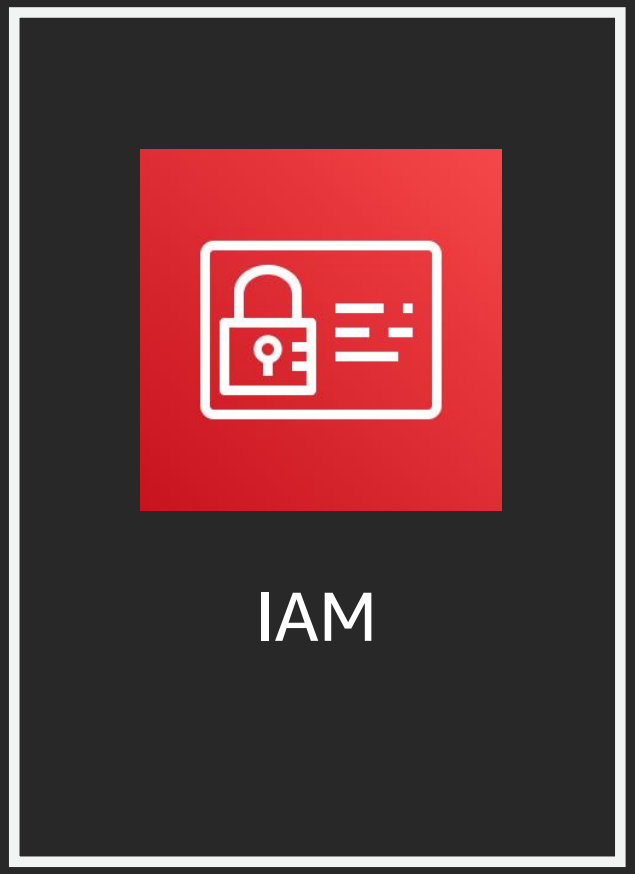
aws | intel

Shared responsibility model



aws | intel

AWS Identity and Access Management (IAM)



- Securely control access to your AWS resources
- Assign granular permissions to users, groups, or roles
- Share temporary access to your AWS account
- Federate users in your corporate network or with an internet identity provider

aws | intel

IAM components

Create

Users
A person or application that interacts with AWS

Groups
Collection of users with identical permissions

Roles
Temporary privileges that an entity can assume

Permissions

Policies

IAM

Defines permissions to control which AWS resources users can access

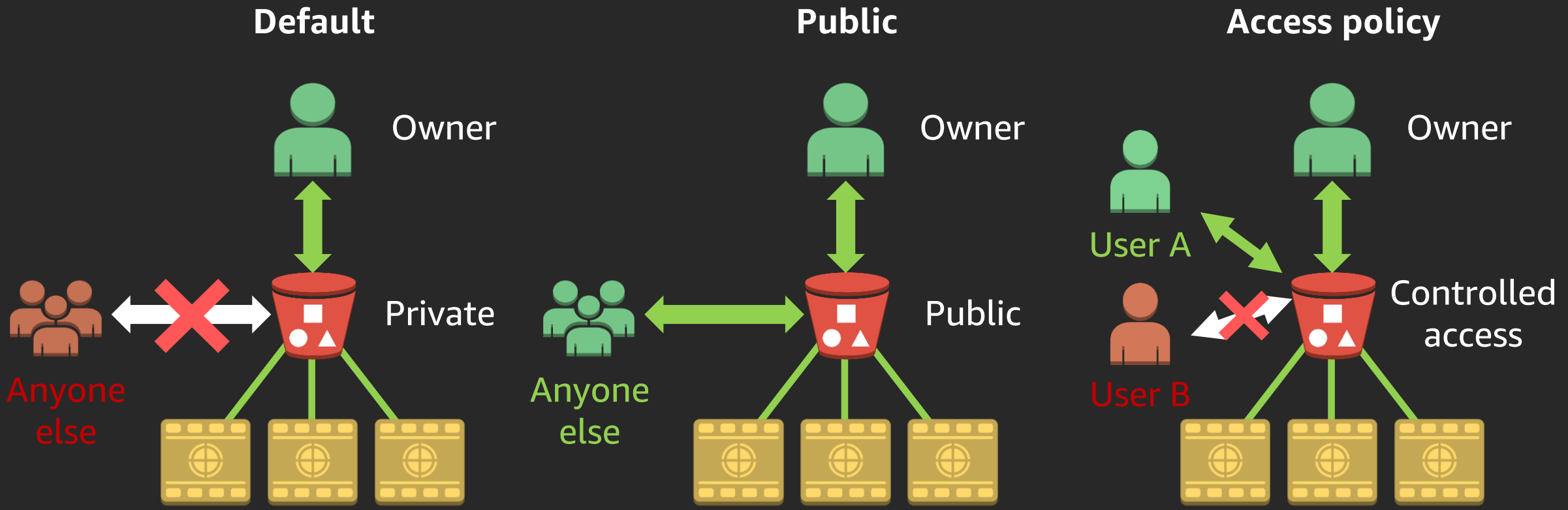
Helps you to meet identity and access control standards

- Authentication
- Authorization

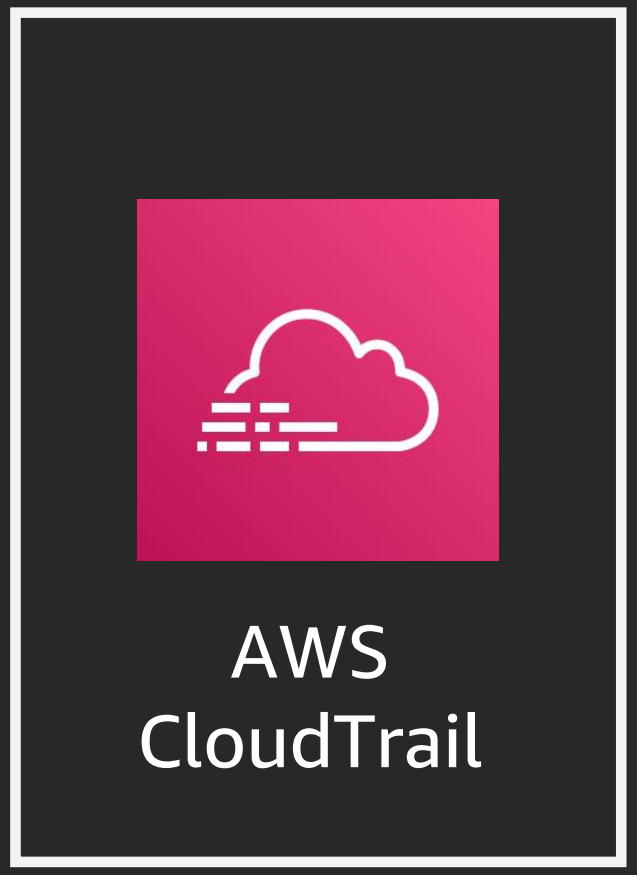
aws | intel

Amazon S3 access control: General

Some services support resource-based policies, such as S3 bucket policies



AWS CloudTrail



- Track user activity and API usage in your AWS account
- Continuously monitor user activities and record API calls
- Useful for compliance auditing, security analysis, and troubleshooting
- Log files are delivered to Amazon S3 buckets

API security-relevant information

What is AWS Trusted Advisor?

A service providing guidance to help you reduce cost, increase performance, and improve security.

Thank you for attending AWSome Day Online Conference

We hope you found it interesting! A kind reminder to **complete the survey.**
Let us know what you thought of today's event and how we can improve the event experience for you in the future.


aws-apj-marketing@amazon.com


twitter.com/AWSCloud


facebook.com/AmazonWebServices


youtube.com/user/AmazonWebServices


linkedin.com/company/amazon-web-services


twitch.tv/aws

Test your knowledge

Thank you!