Connecting Networks in AWS

My company is expanding its Infrastructure on AWS and needs to connect EC2 instance in one VPC with other. It also wants a secure way to connect multiple VPCs and an on-premises network ?

Network Connectivity Dilemma

Scenario Introduction

What is AWS VPC Peering & AWS VPN ?

What are the key considerations when deciding between AWS VPC Peering and AWS VPN for network connectivity within AWS and to on-premises infrastructure ?

Choosing the Right Connectivity

What is AWS VPC Peering:

By default VPC are an isolated environment. EC2 instance in one cannot communicate with another EC2 instance which is in a different VPC

Usecase 🟥 Simple setup, enables direct VPC-to-VPC communication(traffic is route between two VPC’s and this can be in different AWS accounts or different regions), cost-effective for inter-VPC traffic.

Remember 🟥 Doesn't support transitive routing relationships between VPCs.

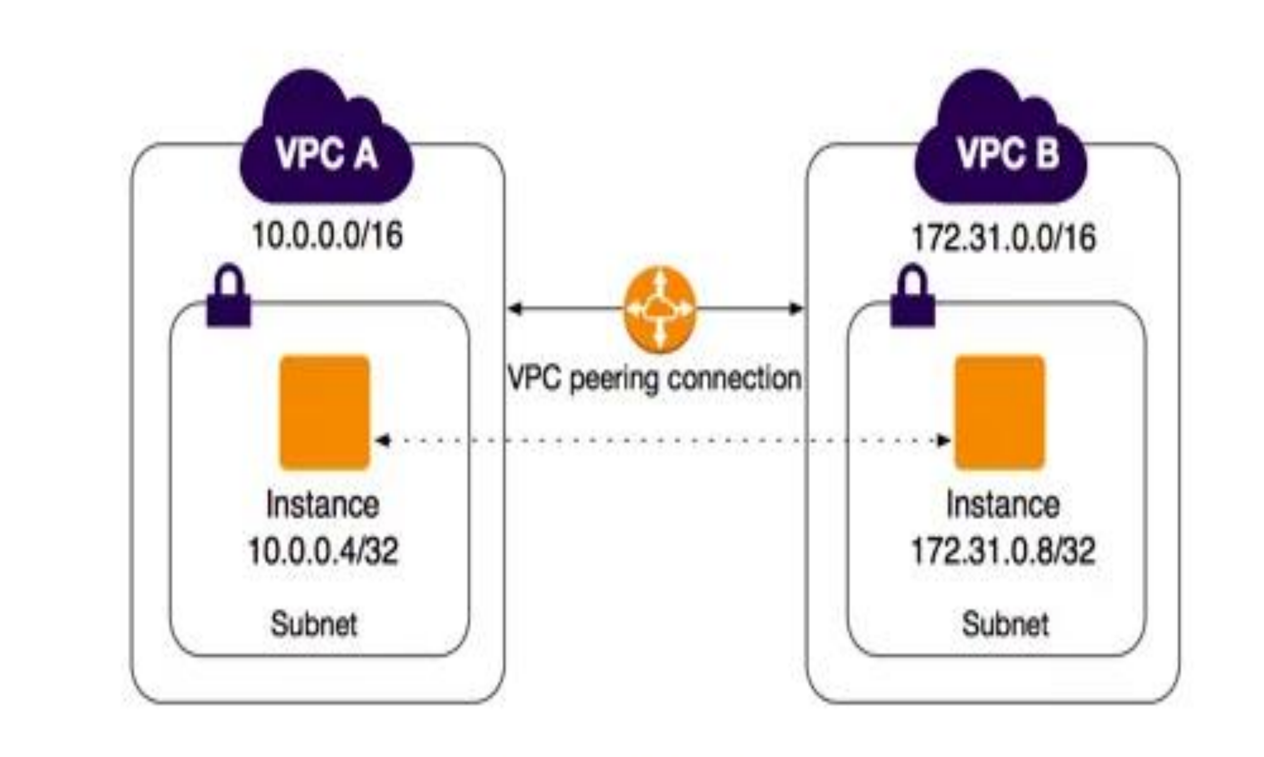


Fig:- VPC Peering

Choosing the Right Connectivity

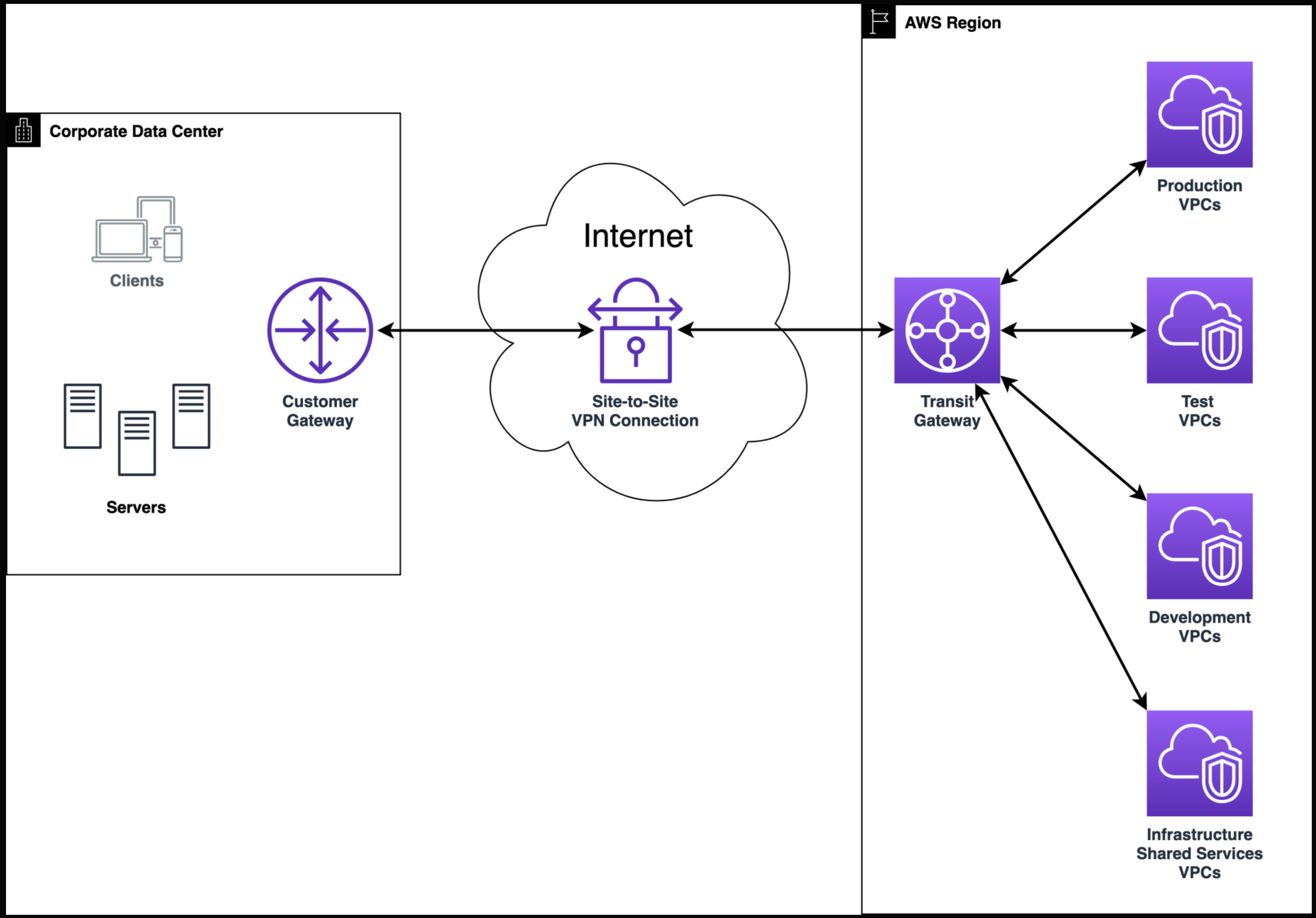
What is AWS VPN (Virtual Private Network)

Use-case:

Secure encrypted connection, supports connecting VPCs across different regions or to an on-premises network, enables transitive routing.

Cons:

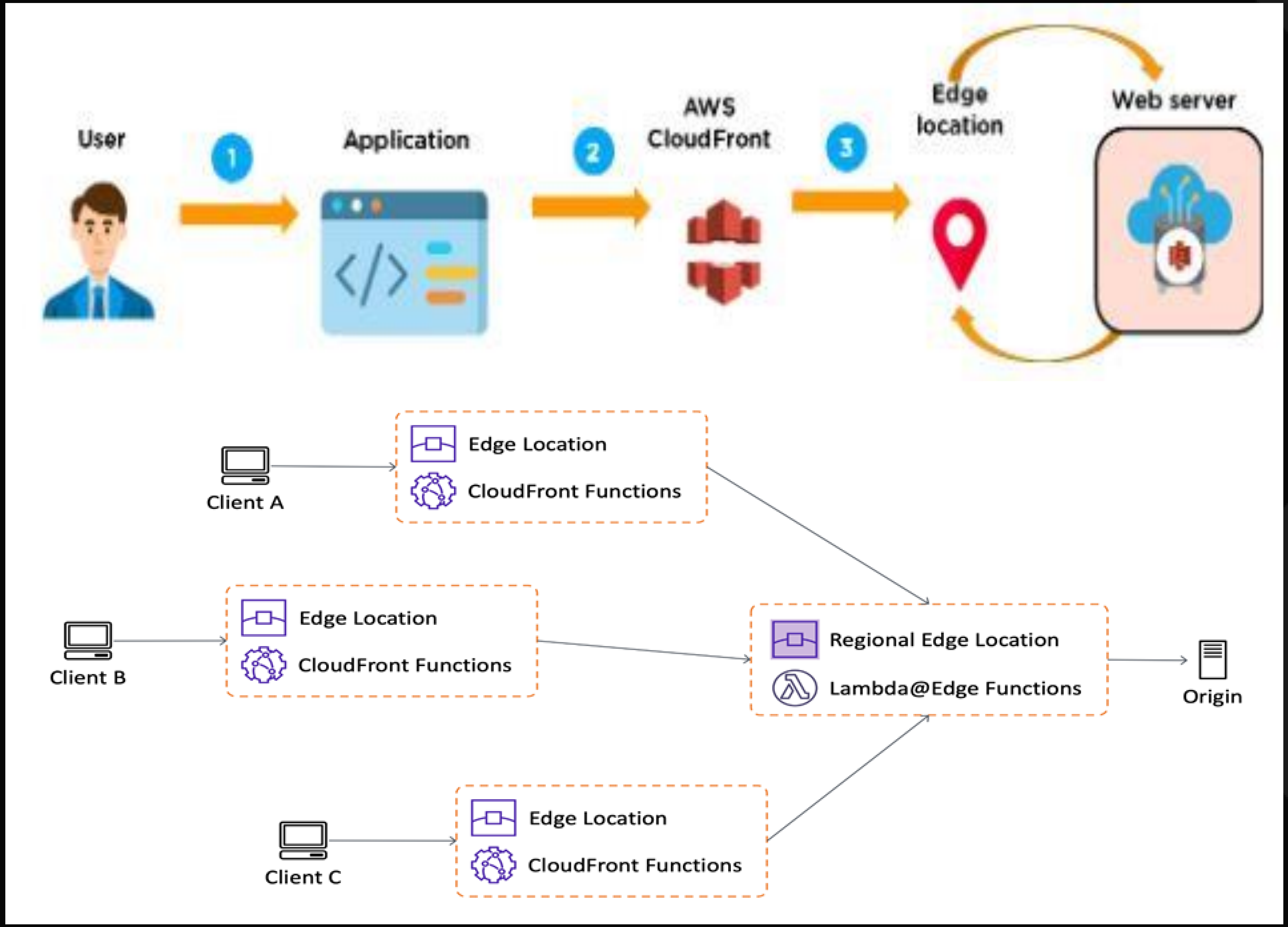
Involves more configuration, higher cost for data transfer.



How Can We Accelerate Global Content Delivery ?

My company has branches all over the globe and wants to set up an online training portal to enrich in-house expertise and technical experience using video tutorials. However, the challenge lies in ensuring fast delivery and optimal performance and security for this system. How can we achieve this efficiently ?

Delivering Global Training Content Seamlessly



What is AWS CloudFront

Distributed Edge Locations: CloudFront delivers content from edge locations globally, reducing latency and providing a layer of protection by shielding origin servers from direct access.

Enhancing Availability and Security with AWS CloudFront

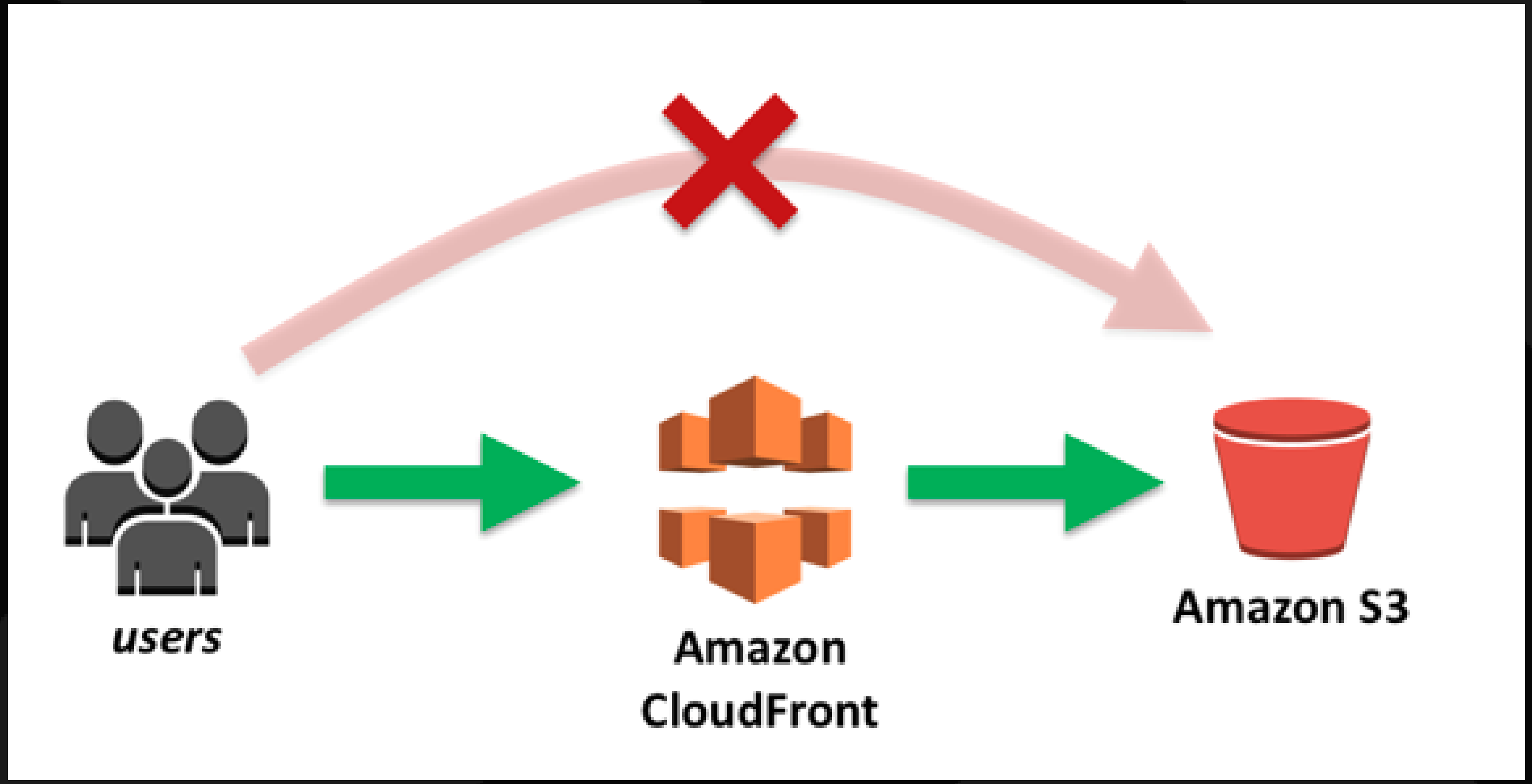
- SSL/TLS Support: CloudFront supports SSL/TLS encryption, ensuring secure communication between users and the content they access.

- DDoS Protection: CloudFront integrates with AWS Shield, providing protection against various DDoS attacks and mitigating potential threats closer to the edge.

- Web Application Firewall (WAF): CloudFront can be paired with AWS WAF, allowing the creation of custom rules to filter malicious traffic before it reaches your application.

AWS CloudFront & Security Enhancements

Example: A company hosts its web application with sensitive user data. By using AWS CloudFront, they distribute their content across edge locations, enabling faster delivery while benefiting from SSL/TLS encryption and AWS Shield DDoS protection, thereby fortifying their application's security.



AWS Security Monitoring Tools

Scenario Introduction

Your company aims to enhance its AWS security posture and needs guidance on choosing the appropriate security monitoring tool

AWS GuardDuty or AWS CloudWatch ?

Security Monitoring Dilemma

Scenario Question

When comparing AWS GuardDuty and AWS CloudWatch, what are the primary differences and best-use scenarios for each tool in bolstering AWS security?

Leveraging Security Monitoring Tools

Scenario Answer

AWS GuardDuty:

- What it is : It is a continuous security monitoring service.Analyses following data sources – VPC flow logs,AWS Cloud trail eventlogs, DNS logs. Not enabled by default
- What it does: Threat detection service, identifies unusual behaviors and potential security threats using machine learning, easy to set up.
- It does that with the help of existing threat intelligence feeds and lists that contain malicious IP's and domains such as Escalation of privileges, EC2 instances having malware, communication with malicious IPs,URL's
- Best Use: Ideal for continuous monitoring and threat detection across AWS accounts.

Cont

Leveraging Security Monitoring Tools

AWS CloudWatch

- Pros: Metrics and log monitoring service, monitors system-wide performance, collects and tracks log files.
- Best Use: Great for monitoring performance, setting alerts, and centralizing log data but less focused on threat detection.

AWS Config OR AWS Systems Manager

Scenario Introduction

Your organization is exploring AWS services to efficiently manage and monitor AWS resources.

Resource Management Tools Comparison

Scenario Introduction

What are the key differences between AWS Config and AWS Systems Manager in terms of resource management and monitoring within AWS?

Resource Management Tools Breakdown

Scenario Answer

AWS Config:

- Functionality: Provides a detailed inventory of AWS resources and tracks configuration changes over time.
- Compliance Monitoring: Evaluates resource configurations against predefined rules to ensure compliance and generates alerts for non-compliant resources.

Example Use Case: A company uses AWS Config to maintain an audit trail of all resource changes made within their AWS environment, ensuring compliance with industry standards.

Resource Management Tools Breakdown

Scenario Answer - cont

AWS Systems Manager:

- Functionality: Offers a suite of tools for resource management, including automation, patch management, and session manager for remote access.
- Automation: Allows for automated resource configuration and management tasks across multiple AWS accounts and regions.
- Example Use Case: An organization employs AWS Systems Manager to automate the patching of its EC2 instances, ensuring security compliance without manual intervention.

Comparison: While AWS Config primarily focuses on configuration history and compliance monitoring, AWS Systems Manager offers a broader set of tools for automation and management tasks.

Thank You