



**CODESTAR**

# **Security**

CodeStar Academy

# Nội dung chính

Encryption

Security



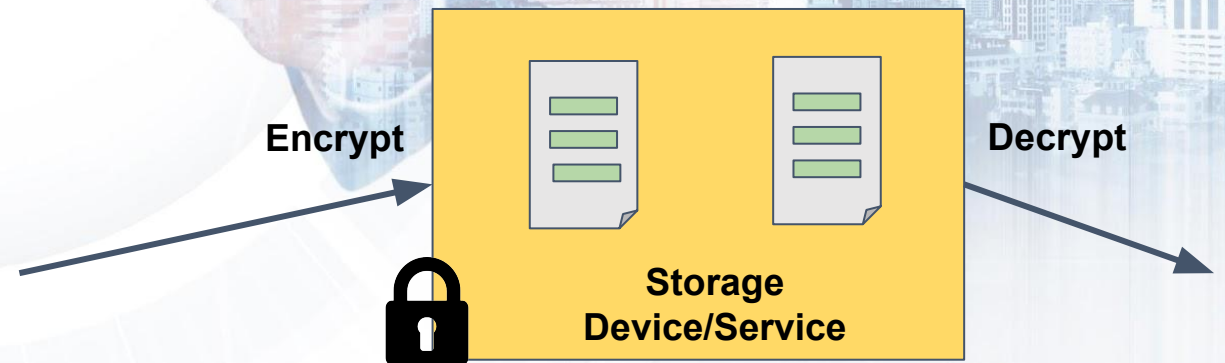
# CODESTAR

# Các kiểu mã hóa căn bản

- Encryption in transit



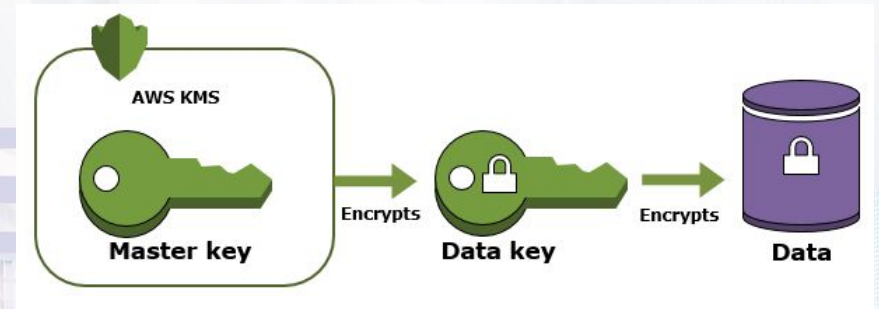
- Encryption at rest



# Các dịch vụ mã hóa căn bản

## AWS KMS (Key Management Service)

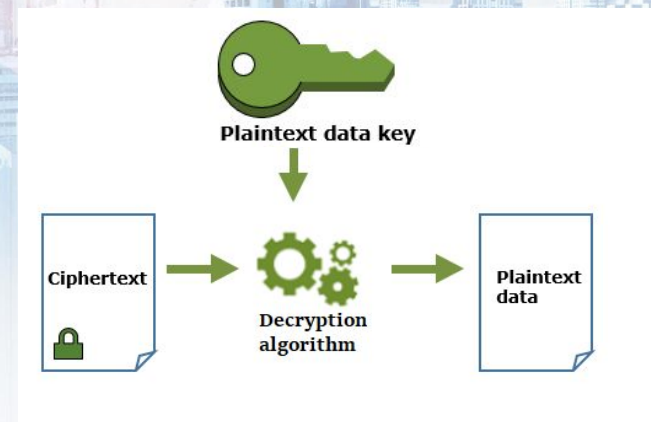
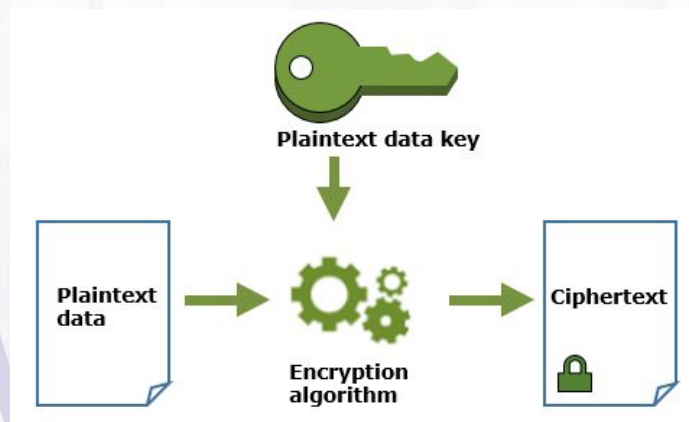
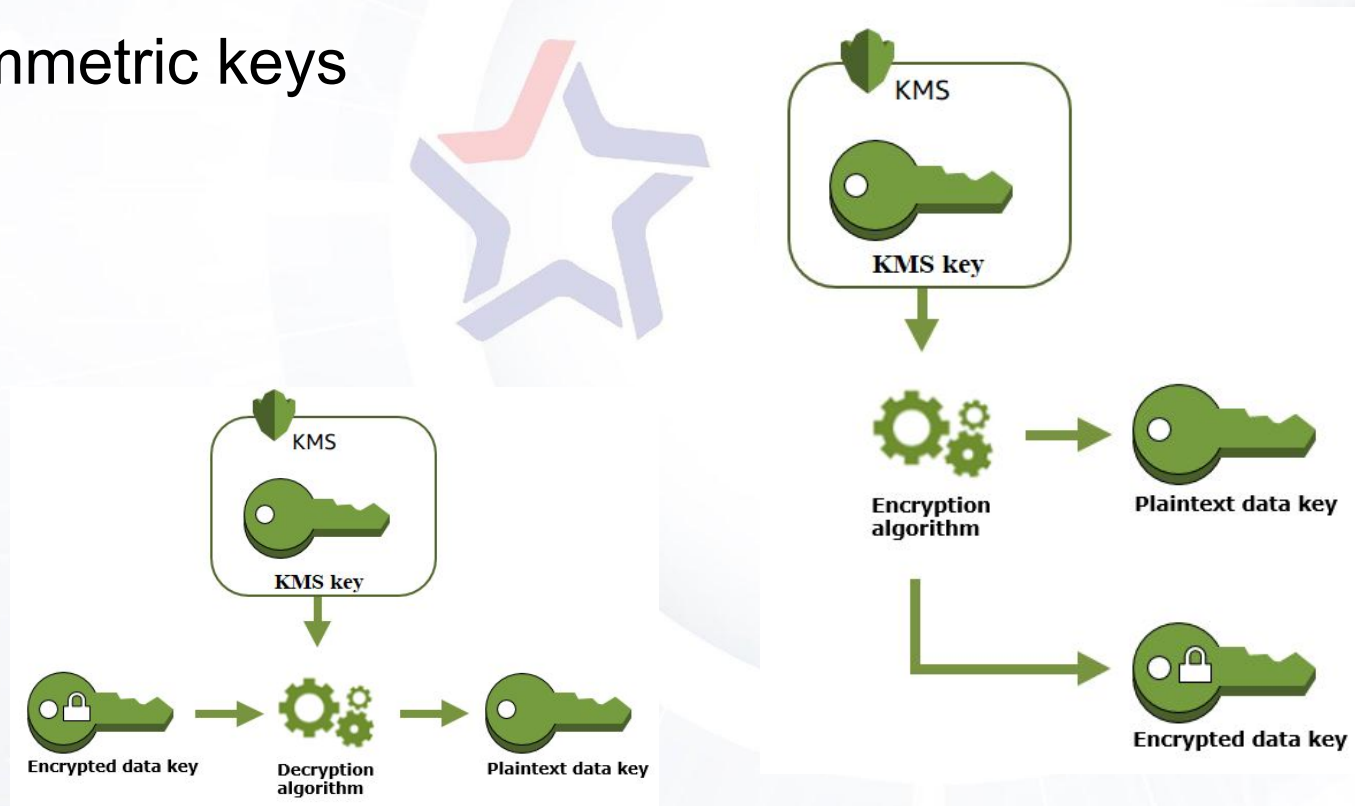
- Là service Region level
- Tạo, lưu trữ và quản lý các keys
- Hỗ trợ mã hóa đối xứng (symmetric) và mã hóa bất đối xứng (asymmetric)
- Hỗ trợ mã hóa (encrypt) và giải mã (decrypt)



# Các dịch vụ mã hóa căn bản

## AWS KMS (Key Management Service)

Symmetric keys

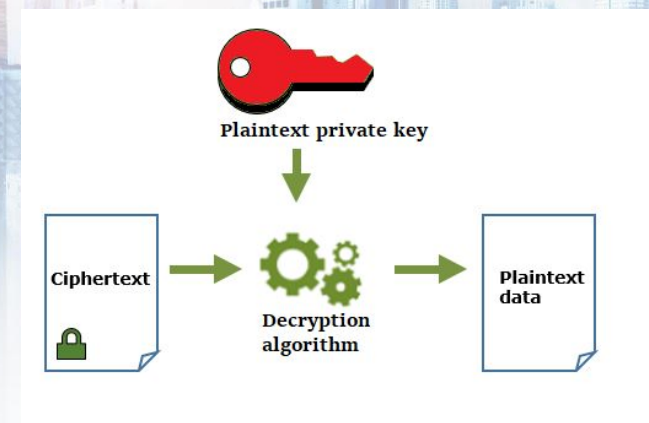
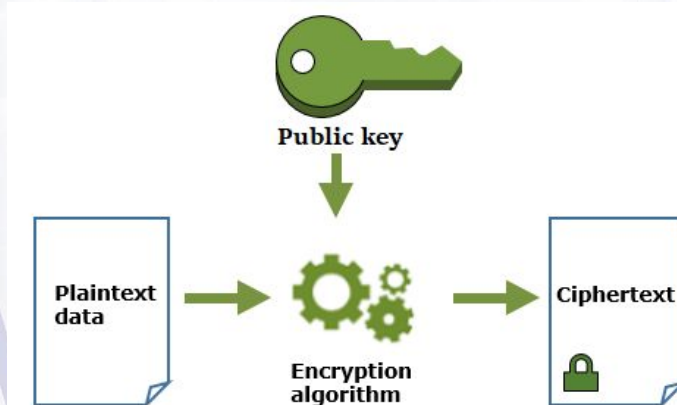
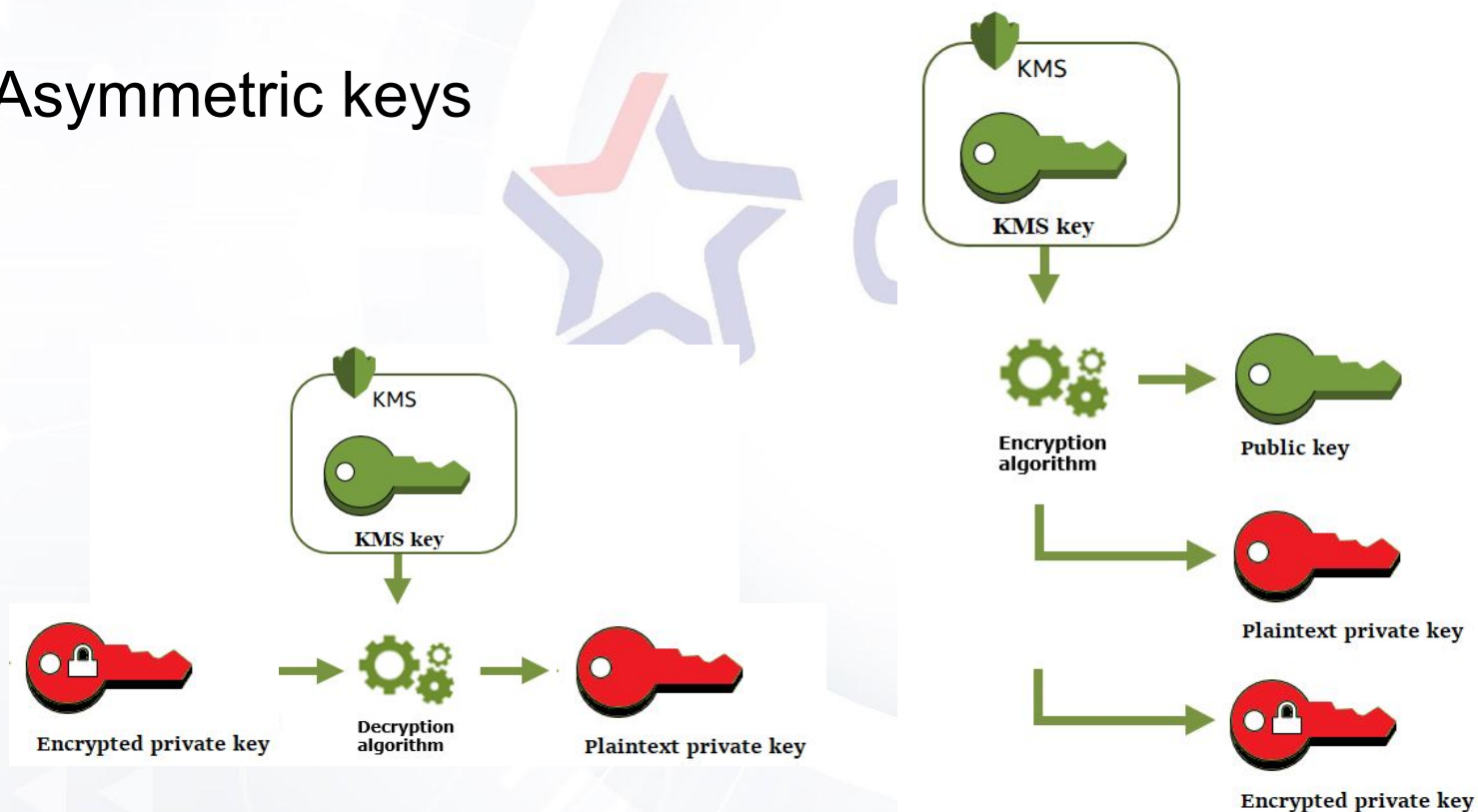




# Các dịch vụ mã hóa căn bản

## AWS KMS (Key Management Service)

Asymmetric keys

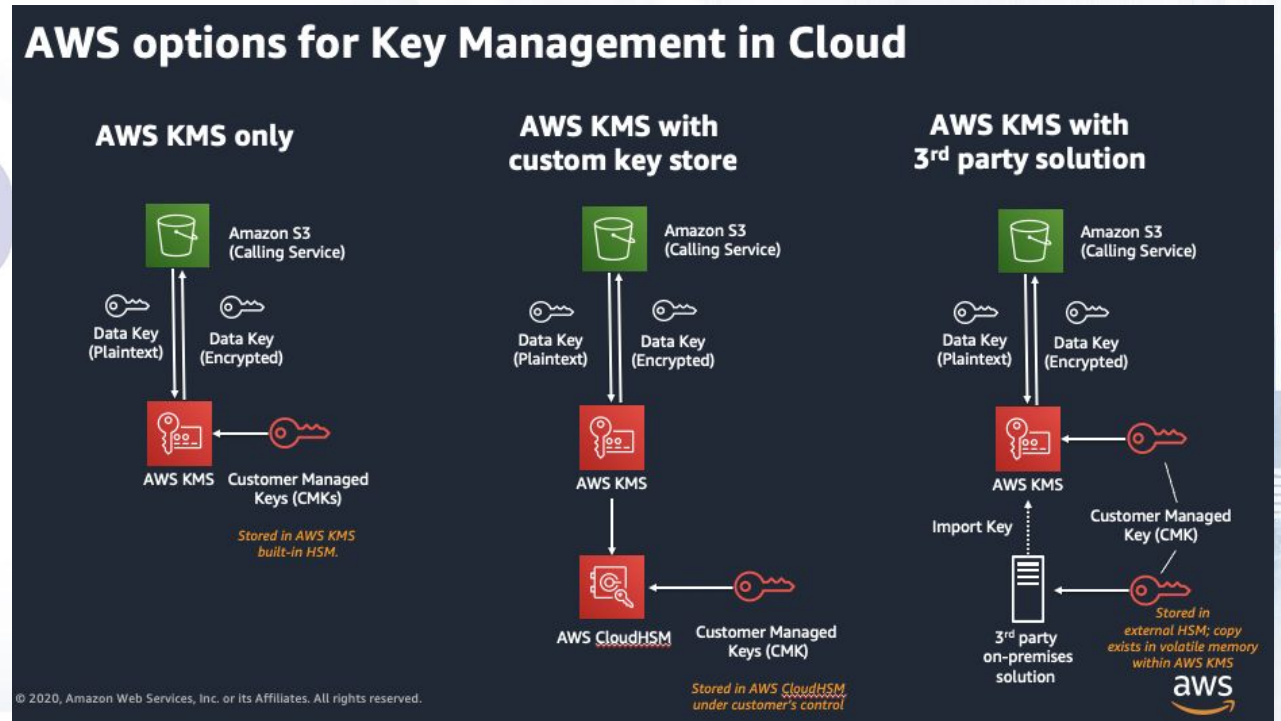


# Các dịch vụ mã hóa căn bản

## AWS KMS (Key Management Service)

Use case:

- Amazon Managed Keys
- Customer Managed Keys
- Custom key store (sử dụng kèm CloudHSM)



# Các dịch vụ mã hóa căn bản

## AWS KMS (Key Management Service)

So sánh các loại

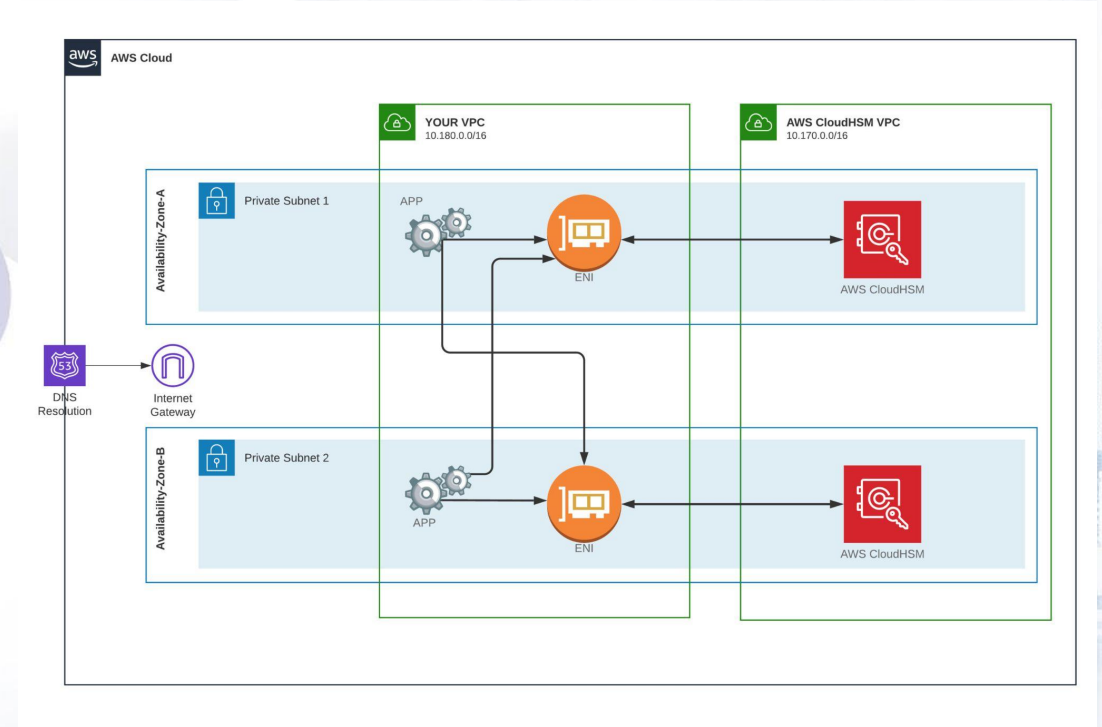
Type of KMS key	Can view KMS key metadata	Can manage KMS key	Used only for my AWS account	Automatic rotation	Pricing
Customer managed key	Yes	Yes	Yes	Optional. Every year (approximately 365 days)	Monthly fee (pro-rated hourly) Per-use fee
AWS managed key	Yes	No	Yes	Required. Every year (approximately 365 days)	No monthly fee Per-use fee (some AWS services pay this fee for you)
AWS owned key	No	No	No	Varies	No fees



# Các dịch vụ mã hóa căn bản

## AWS CloudHSM (Hardware Security Module)

- Là một thành phần phần cứng, lưu trữ key.
- Thường được sử dụng kết hợp với KMS



# Các dịch vụ hỗ trợ Security

## AWS Shield

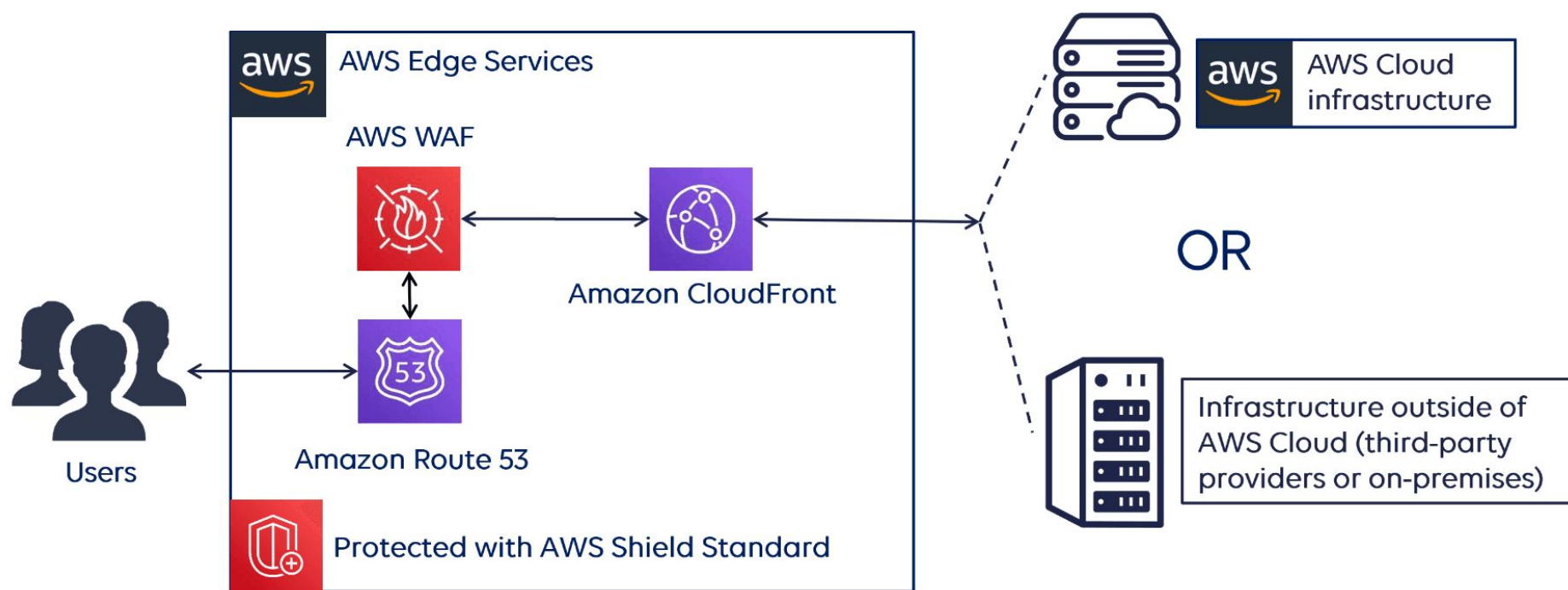
- Dịch vụ hỗ trợ bảo vệ người dùng khỏi tấn công DDoS.
- Có 2 chế độ AWS Shield Standard (Free, apply cho tất cả người dùng AWS) và AWS Shield Advanced (có 1 số tính năng đặc biệt)



**AWS Shield**

# Các dịch vụ hỗ trợ Security

## AWS Shield Standard



# Các dịch vụ hỗ trợ Security

## AWS Shield Advanced

### DDoS protection with AWS Shield

#### Standard



Available for all AWS clients without additional charge

- Protection against common attacks (SYN/UDP Floods, Reflection Attacks, etc. Layer 3/4)
- Automatic detection and mitigation

#### Advanced



Charged service that provides additional protection against more complex attacks

- Protection against advanced attacks (Layer 7)
- 24x7 DDoS response team
- Cost Protection
- Better monitoring / Visualization

© 2020, Amazon Web Services, Inc. or its Affiliates.

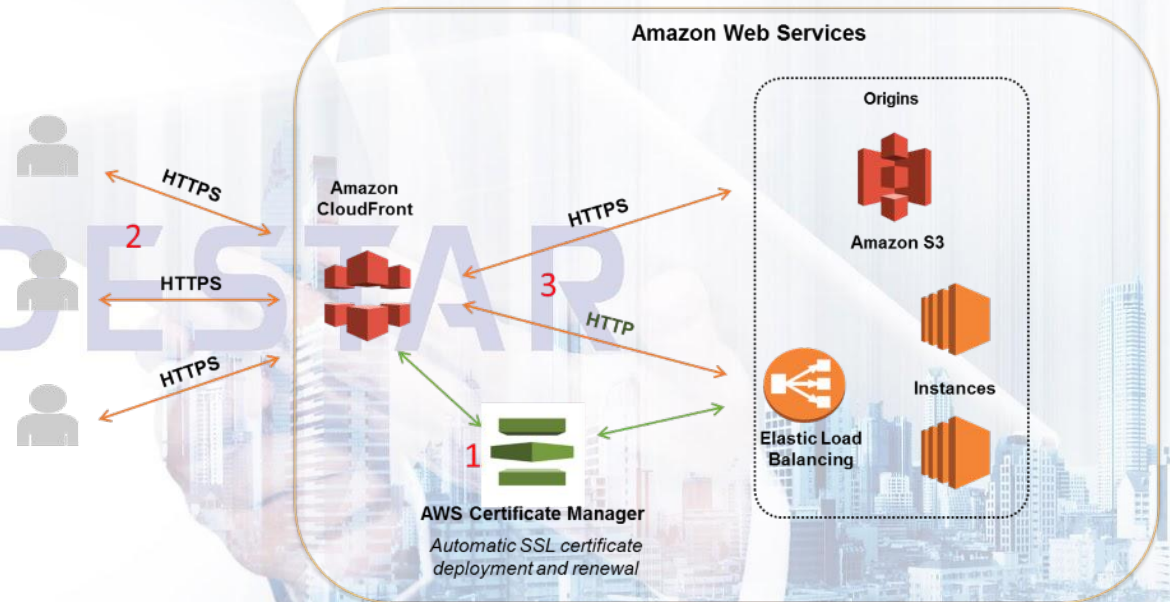




# Các dịch vụ hỗ trợ Security

## ACM (AWS Certificate Manager)

- Service hỗ trợ khởi tạo, quản lý, deploy các certificate SSL, TLS cho các resource nội bộ.
- ACM có hỗ trợ upload certificate từ 1 bên thứ 3

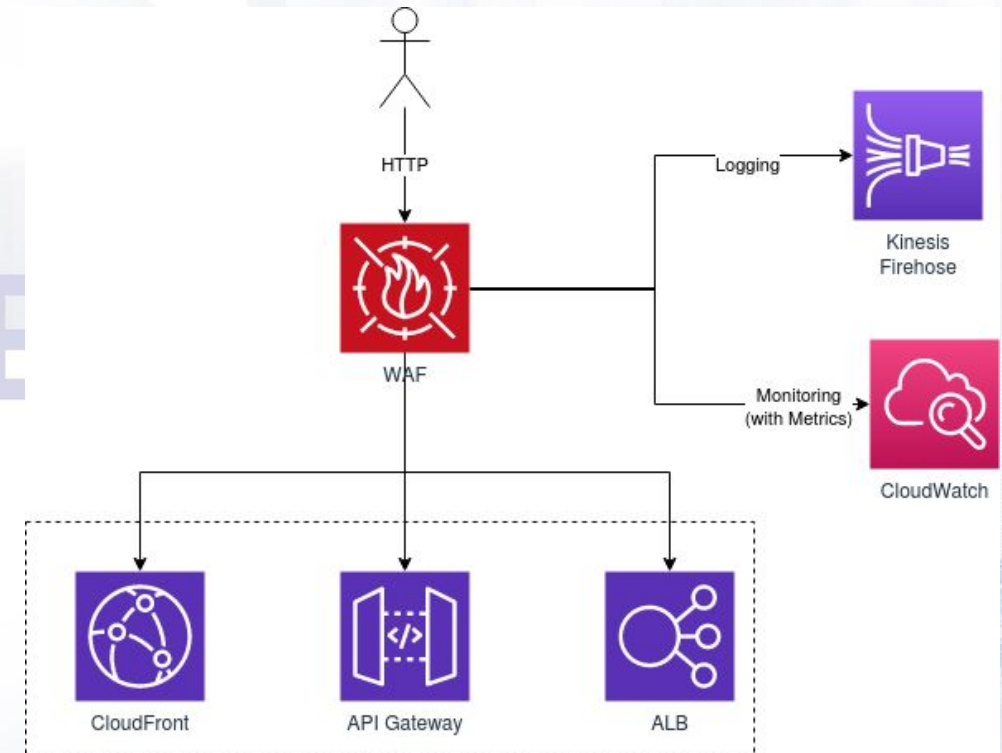




# Các dịch vụ hỗ trợ Security

## WAF (Web Application Firewall)

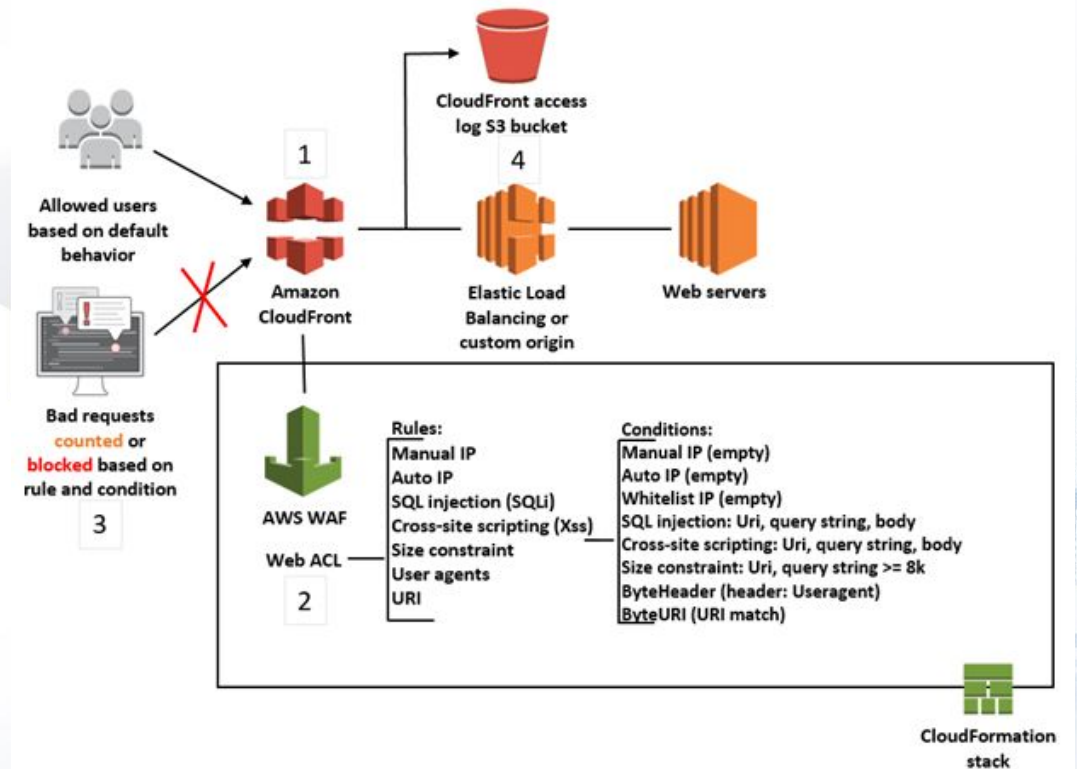
- Bảo vệ hệ thống khỏi những loại tấn công thường gặp (SQL Injection, XSS, ...)
- Có thể Add vào:
  - + CloudFront
  - + API GW
  - + ALB
  - + Cognito pool



# Các dịch vụ hỗ trợ Security

## WAF (Web Application Firewall)

- Web ACL định nghĩa ra các Rule/RuleGroup hỗ trợ filter/delete hoặc allow những request match rule.
- Web ACL có thể sử dụng các thông tin ở Layer 7 để allow hay block các request.





# THANK YOU