ELB

🗺️ ELB Learning Roadmap

🎯 **Roadmap học ELB từ cơ bản đến nâng cao**

1. **Foundation** → Khái niệm Load Balancer, các loại ELB
2. **ALB Deep Dive** → Routing, Target Groups, Security
3. **NLB Deep Dive** → TCP/UDP, Performance, Static IP
4. **Advanced Concepts** → Cross-Zone LB, SSL/TLS, SNI
5. **Integration** → ASG, Multi-AZ, HA Architecture
6. **Best Practices** → Security, Reliability, Cost Optimization

---

▼ 📚 1. Load Balancer Fundamentals

Khái niệm cơ bản

Load Balancer là dịch vụ phân phối traffic đến nhiều targets (EC2, containers, IP addresses) để tăng availability và fault tolerance.

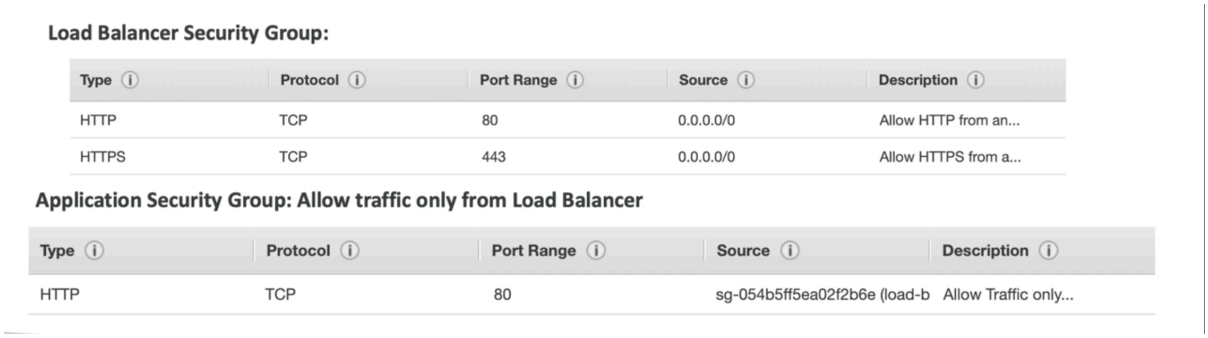
4 loại Load Balancer trong AWS

- Classic Load Balancer (v1 - old generation) – 2009 – CLB
  - HTTP, HTTPS, TCP, SSL (secure TCP)
- Application Load Balancer (v2 - new generation) – 2016 – ALB
  - HTTP, HTTPS, WebSocket
- Network Load Balancer (v2 - new generation) – 2017 – NLB
  - TCP, TLS (secure TCP), UDP
- Gateway Load Balancer – 2020 – GWLB
  - Operates at layer 3 (Network layer) – IP Protocol

Loại	Layer	Protocol	Use Case
ALB	Layer 7	HTTP/HTTPS/gRPC	Web applications, microservices
NLB	Layer 4	TCP/UDP/TLS	Ultra-low latency, static IP, millions RPS
GLB	Layer 3	IP	Third-party appliances, security
CLB	Layer 4/7	HTTP/TCP	Legacy (EC2-Classic)

⚠️ **Recommended:** Sử dụng ALB cho web applications và NLB cho non-HTTP workloads. CLB đang được deprecated.

Security Group Rules Pattern



Load Balancer Security Group:

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	Allow HTTP from an...
HTTPS	TCP	443	0.0.0.0/0	Allow HTTPS from a...

Application Security Group: Allow traffic only from Load Balancer

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	sg-054b5ff5ea02f2b6e (load-b	Allow Traffic only...

Best Practice:

- **Load Balancer SG:** Chỉ cho phép ports **80** và **443** từ Internet
- **Application SG:** Chỉ cho phép port **80** từ **source là Load Balancer SG**

▼ 🔷 2. Application Load Balancer (ALB)

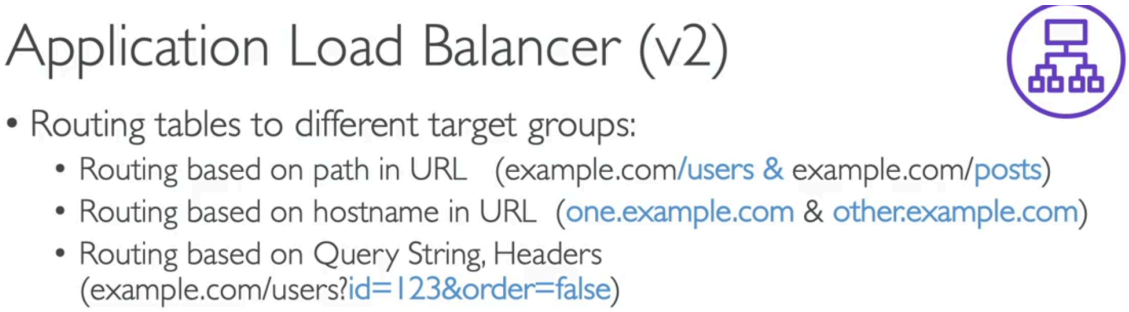
Tính năng chính

ALB hoạt động ở **Layer 7** (Application Layer), hỗ trợ:

- **HTTP/HTTPS/gRPC** protocols
- **WebSocket & HTTP/2** support

ALB filters:

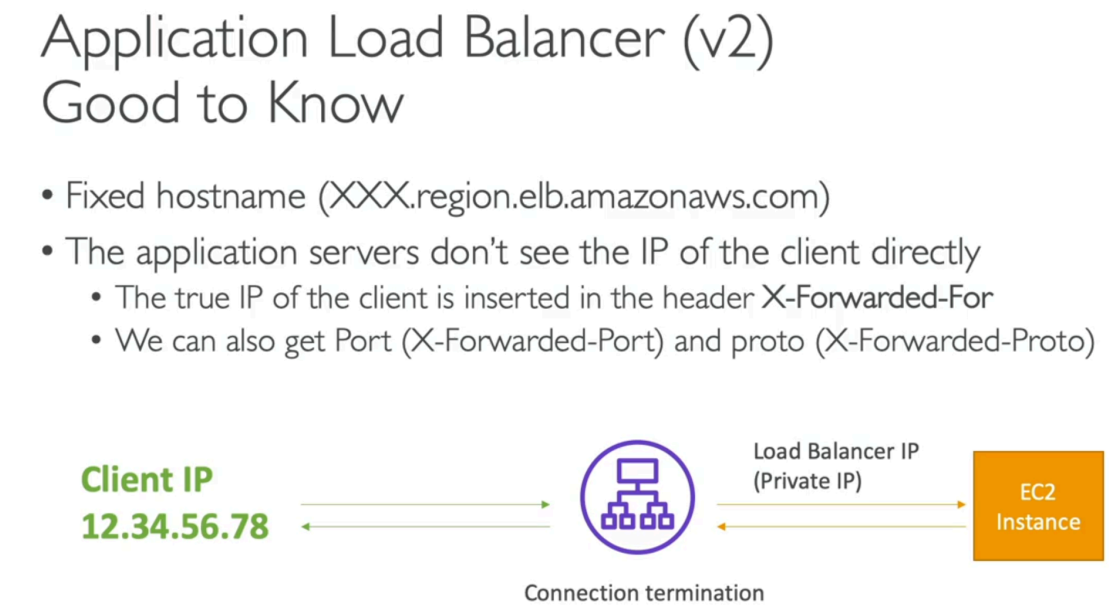
- **Path-based routing:** `/api/*` → API servers, `/images/*` → Image servers
- **Host-based routing:** `api.example.com` vs `www.example.com`
- **Query string & header routing**



ALB typical scenarios:

- Microservices architecture
- Container-based applications (ECS/EKS)
- Lambda functions as targets
- Multiple applications behind single ALB

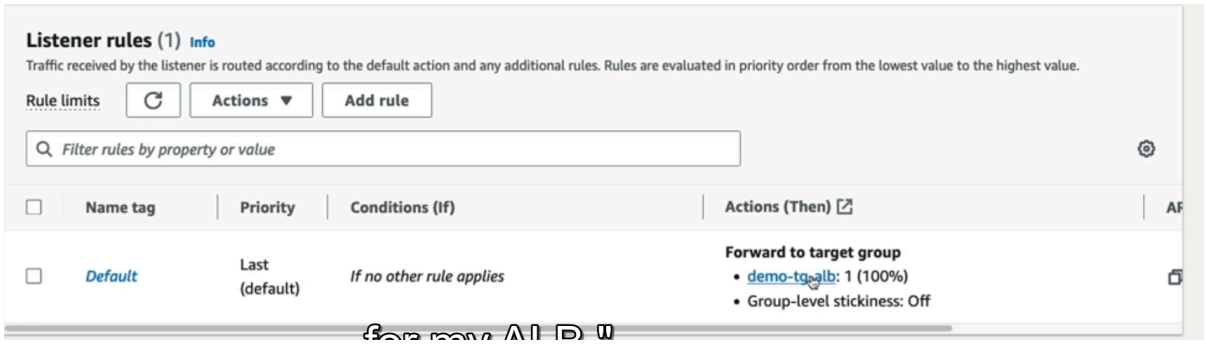
Request Headers



Important Headers:

- **X-Forwarded-For:** Client IP address
- **X-Forwarded-Port:** Client port (80 or 443)
- **X-Forwarded-Proto:** Protocol (HTTP or HTTPS)

Default Target Group



Default routing: Khi request không match rule nào, ALB sẽ forward đến **default target group**.

usecase: Google chỉ có một ALB route cho nhiều domain

> 💡 **Pattern:** Sử dụng default target group để return 404 page hoặc redirect đến homepage

▼ 💡 Dynamic IPs vs Static IPs trong AWS Load Balancers

Khái niệm

Dynamic IPs là địa chỉ IP có thể thay đổi theo thời gian khi Load Balancer scale hoặc update. **Static IPs** là địa chỉ IP cố định không thay đổi trong suốt vòng đời của resource.

So sánh ALB vs NLB

- **ALB (Application Load Balancer):** Sử dụng **Dynamic IPs**
  - IP addresses thay đổi khi ALB scale out/in để đáp ứng traffic
  - Client connect thông qua DNS name, không phải IP trực tiếp
  - Không thể whitelist IP của ALB trong firewall rules
- **NLB (Network Load Balancer):** Hỗ trợ **Static IP per AZ**
  - Mỗi AZ được assign một Static IP cố định
  - Có thể attach **Elastic IP** (EIP) cho mỗi AZ
  - Cho phép whitelist IP trong firewall, security policies
  - Ideal cho integration với on-premises systems yêu cầu IP whitelisting

Use Cases cho Static IPs

- **Compliance requirements:** Một số regulations yêu cầu whitelist specific IPs
- **Third-party integration:** Partner systems chỉ accept traffic từ whitelisted IPs
- **Firewall rules:** On-premises firewalls cần static IPs để configure rules

- **DNS caching:** Giảm dependency vào DNS resolution với static IPs

> **Best Practice:** Nếu application cần static IPs cho whitelisting hoặc compliance, sử dụng NLB với Elastic IPs. Nếu chỉ cần Layer 7 routing và không cần static IPs, ALB là lựa chọn tốt hơn.

> ✅ **Use Case:** Cần whitelist IP của Load Balancer → dùng NLB với Elastic IP

▼ 🔶 3. Network Load Balancer (NLB)

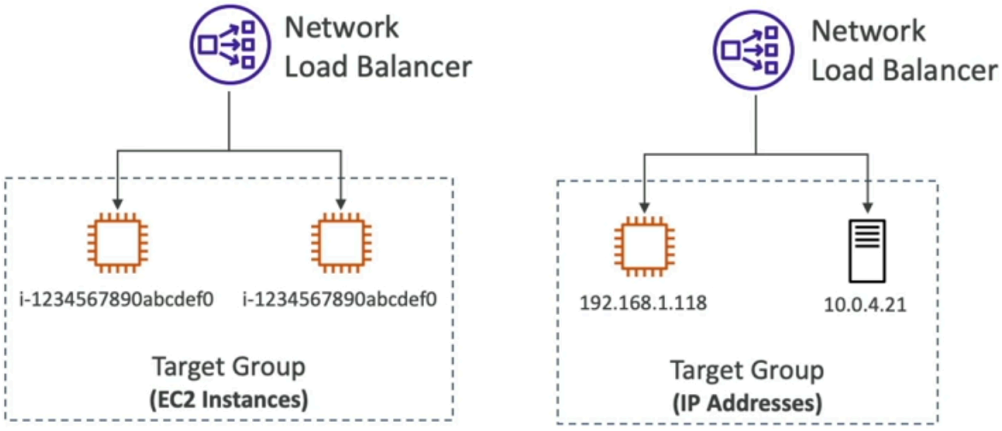
Tính năng chính

NLB hoạt động ở **Layer 4** (Transport Layer):

Lý do sử dụng NLB:[2]

- **Forward TCP & UDP traffic** (không parse HTTP)
- **Ultra-low latency** (microseconds vs milliseconds)
- **Handle millions of requests per second**
- **Static IP per AZ** + Support Elastic IP
- **Preserve source IP** của client

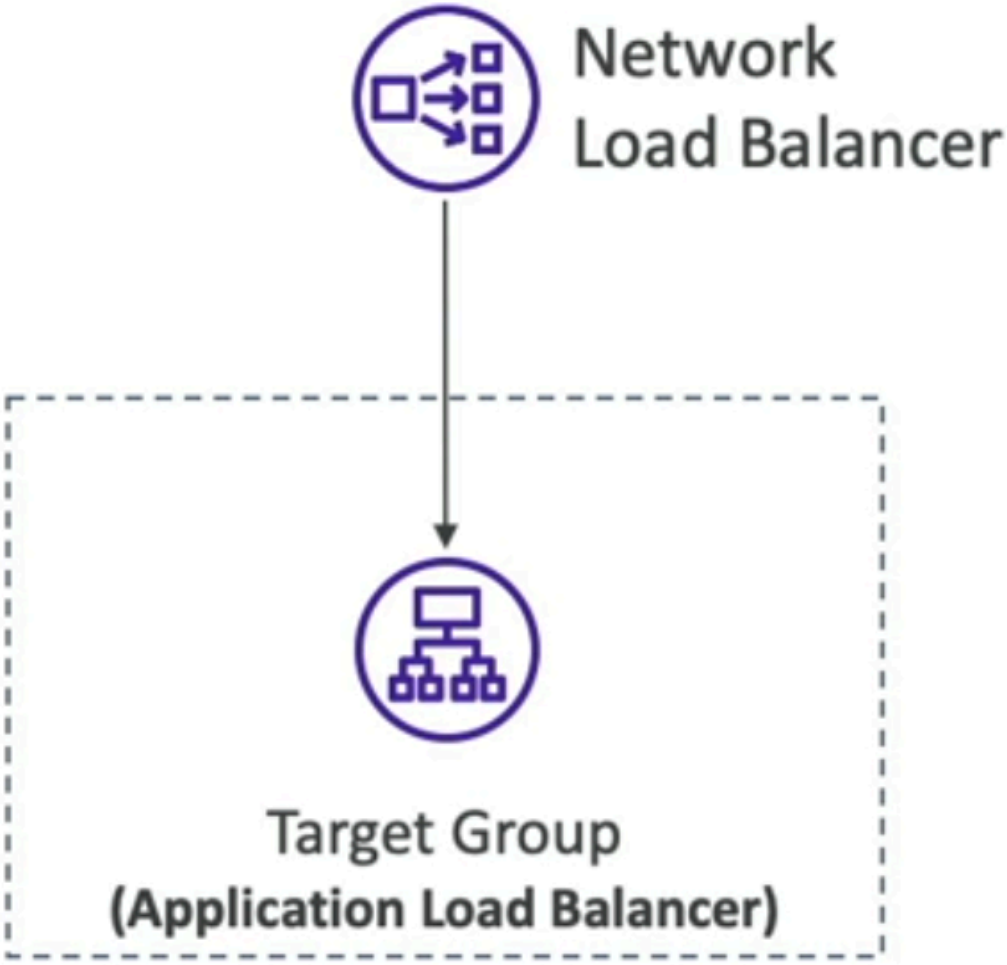
Target Groups của NLB



NLB hỗ trợ target types:

- **EC2 instances**
- **IP addresses** (on-premises servers, containers)
- **Application Load Balancer** (pattern: NLB → ALB)

Pattern: NLB trước ALB



Lợi ích:[2][3]

- Static IP + Elastic IP từ NLB
- Layer 7 routing intelligence từ ALB
- Sử dụng trong NEXON cho **CloudFront replacement** với AWS Shield Advanced

Health Checks

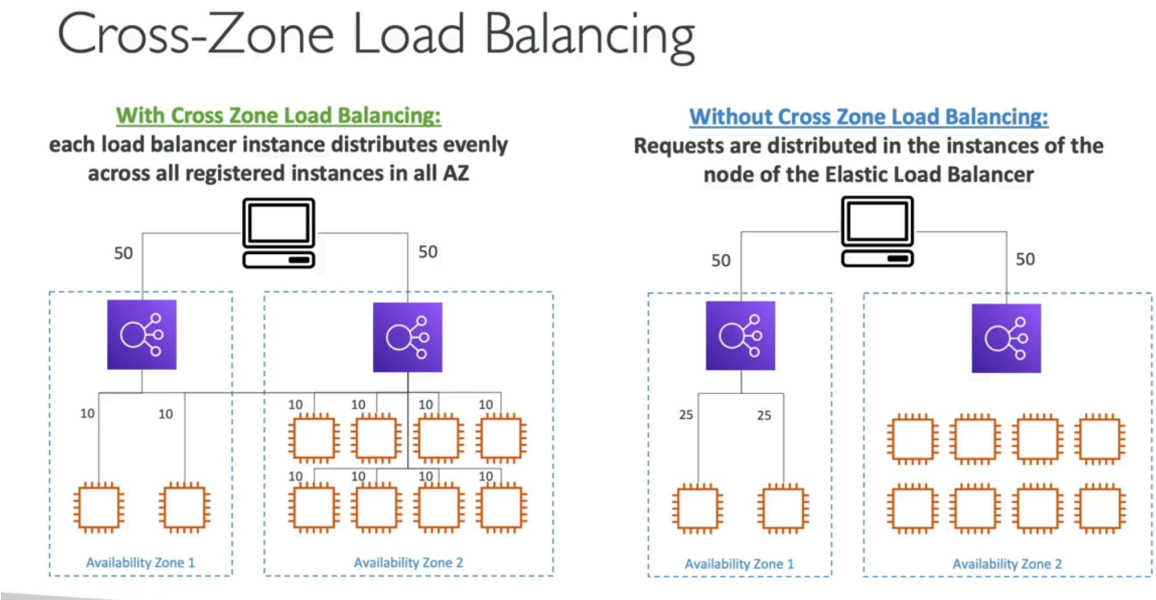
NLB Health Check protocols:

- TCP

- HTTP
- HTTPS

▼ ⚖️ 4. Cross-Zone Load Balancing

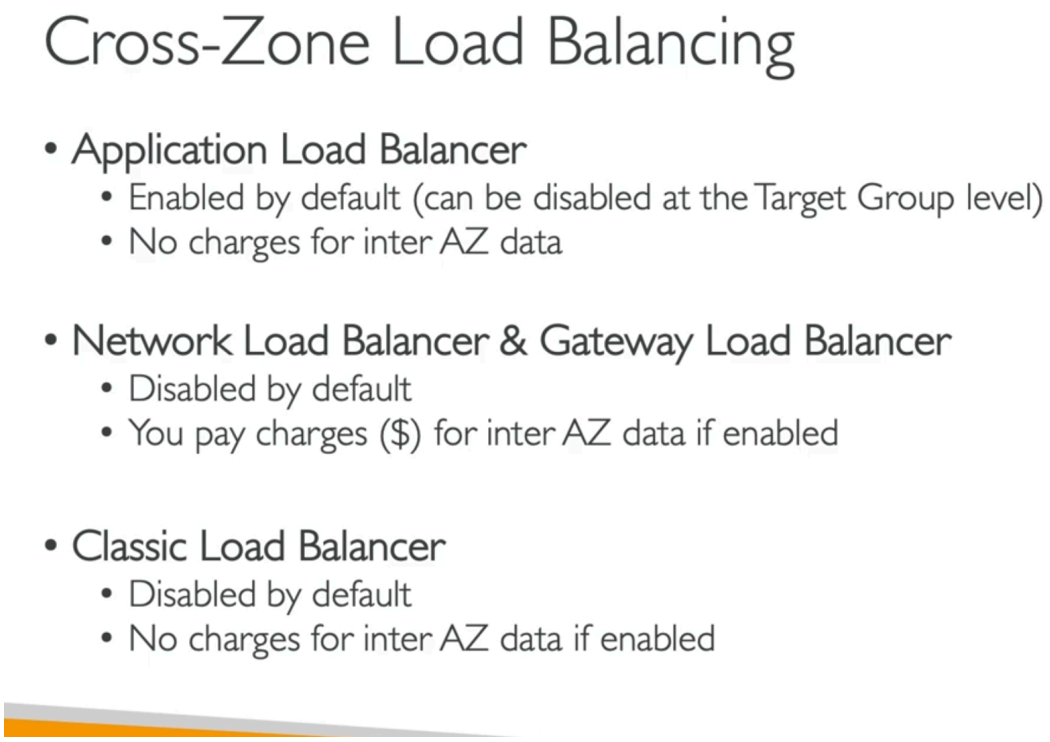
Khái niệm



Hai chế độ:[2]

Mode	Behavior	Traffic Distribution
Cross-Zone Enabled	Phân bổ **đều** traffic cho **tất cả instances** ở **mọi AZ**	50/50 cho mỗi instance
Cross-Zone Disabled	Phân bổ traffic **chỉ trong AZ** của LB node	Không đều giữa các AZ

Pricing Considerations



💰 **Important for Cost:**

- **ALB:** Cross-Zone miễn phí
- **NLB:** Cross-Zone **tính phí** data transfer giữa AZs
- **GLB:** Cross-Zone **tính phí**

▼ 🔒 5. SSL/TLS & Certificate Management

AWS Certificate Manager (ACM)

AWS CM là dịch vụ quản lý TLS certificates:[2]

- **Free** SSL/TLS certificates
- **Auto-renewal**
- Integration với ALB, NLB, CloudFront

Server Name Indication (SNI)

SNI cho phép host **multiple SSL certificates** trên single Load Balancer:

- Client chỉ định hostname trong TLS handshake
- ALB/NLB chọn certificate phù hợp
- **Chỉ hỗ trợ:** ALB, NLB, CloudFront (CLB không support)

> **Best Practice:** Sử dụng HTTPS listeners với ACM certificates. Configure HTTP → HTTPS redirect trên ALB.[4]

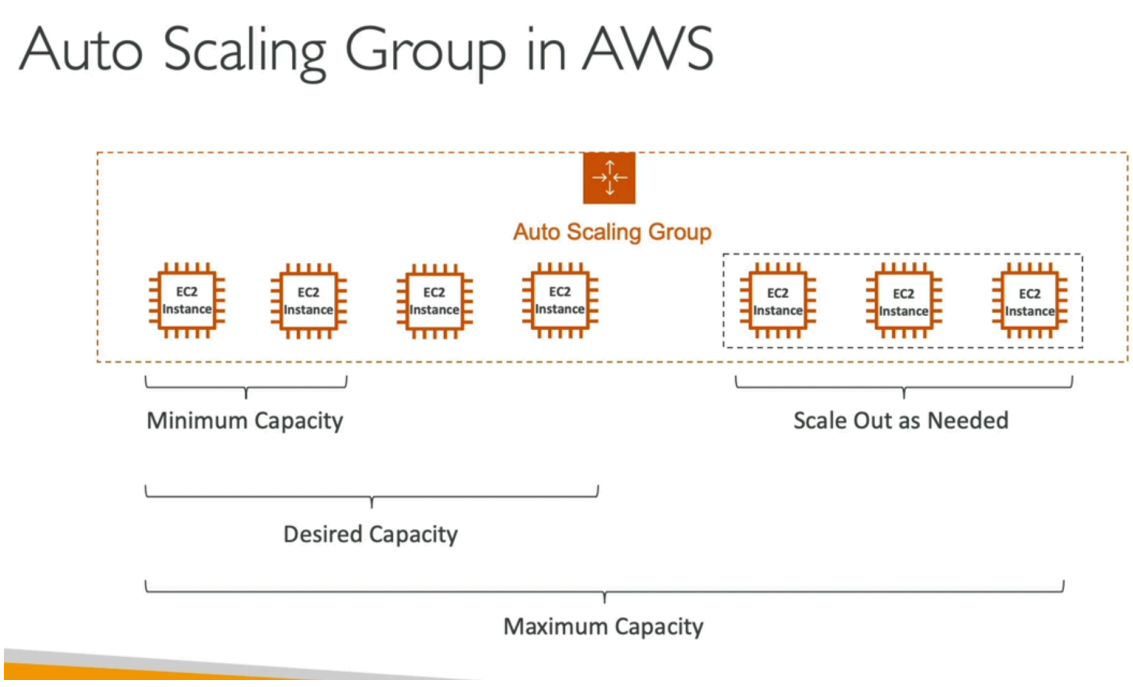
End-to-End Encryption

Pattern:[4]

1. Client → LB: **HTTPS** (TLS termination at LB)
2. LB → Targets: **HTTPS** (re-encryption)

▼ 🔄 6. Integration với Auto Scaling Group

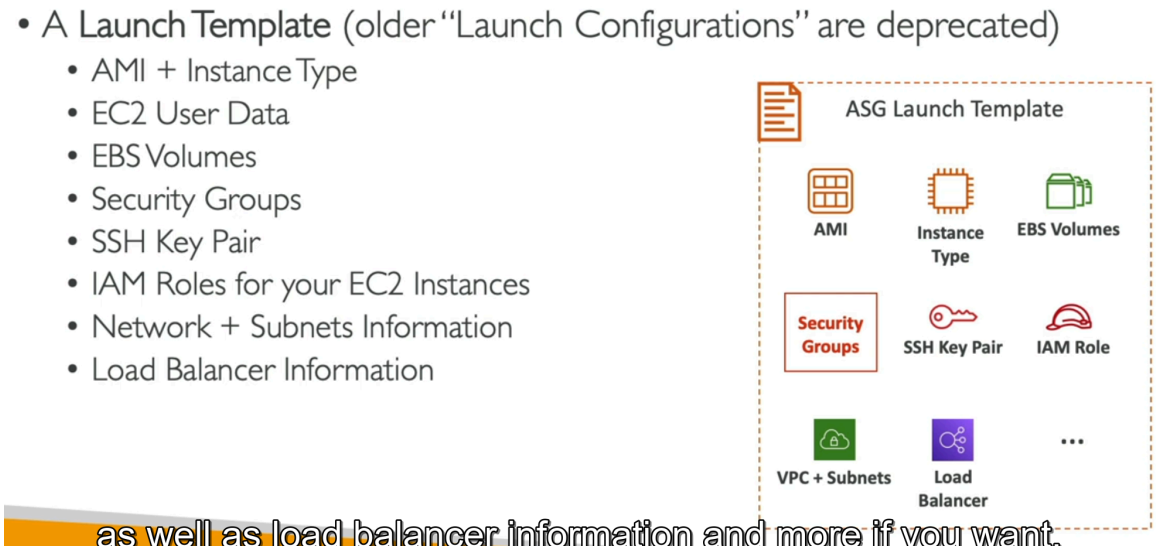
ASG + Load Balancer



Lợi ích:[2]

- LB **tự động register/deregister** instances từ ASG
- Health checks từ LB trigger ASG replacements
- Seamless scaling without manual intervention

Launch Template



Launch Template chứa:

- AMI ID
- Instance type
- Security groups
- User data script
- IAM instance profile

✅ **Optimization Tip:** Sử dụng **AMI** với pre-installed application để giảm initialization time và cooldown period

ASG Scaling Strategies

1. Dynamic Scaling:[2]

▼ **Target Tracking Scaling**

- Simple to set up
- Example: Maintain average CPU at 40%

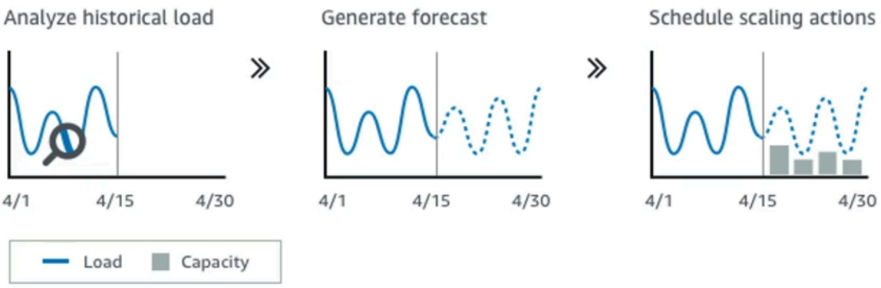
▼ **Simple/Step Scaling**

- CloudWatch alarm triggers scaling
- Example: CPU > 70% → add 2 instances
- Example: CPU < 30% → remove 1 instance

2. Scheduled Scaling:

- Based on predictable patterns
- Example: Scale up to 10 instances at 5 PM on Fridays

• Predictive scaling: continuously forecast load and schedule scaling ahead



✅ **Key Point:** Tất cả ASG strategies đều cần **CloudWatch alarms** để trigger

▼ 🏗️ 7. High Availability Architecture

Multi-AZ Best Practices

AWS Recommended:[5][6]

- **Minimum 2 AZs** for fault tolerance

- **All AZs should have registered targets**
- Enable **DNS failover** (default threshold = 1 healthy target)

> 🎯 **Nexon Pattern:** Route53 → INFACE Gateway → ALB → EKS (Multi-AZ) [7]

Connection Draining

Purpose: Gracefully complete in-flight requests before deregistering target

- **Default:** 300 seconds
- **Range:** 1-3600 seconds

▼ ✨ 8. Best Practices Summary

Security[4]

✅ **Use HTTPS/TLS listeners** trên ALB và NLB

✅ **Enable HTTP → HTTPS redirect** trên ALB

✅ **Use ACM** cho certificate management

✅ **Most restrictive security policy** compatible với clients

✅ **End-to-end encryption:** HTTPS listener + HTTPS target group

Reliability[8]

✅ **Configure minimum 2 AZs** cho Load Balancer

✅ **Register targets in all AZs** được enable

✅ **Enable Cross-Zone Load Balancing** (except khi optimize cost cho NLB)

✅ **Configure appropriate health checks**

✅ **Monitor với CloudWatch metrics**

Monitoring & Logging[4]

✅ **Enable access logs** → S3 bucket

✅ **Consolidate logs** trong Log Archive account

✅ **Monitor AWS Health events**

✅ **Set up CloudWatch alarms** cho key metrics

Cost Optimization

✅ **Choose đúng loại LB** cho use case

✅ **Optimize Cross-Zone LB** cho NLB (tính phí)

✅ **Use capacity reservations** cho predictable traffic spikes

✅ **Right-size target instances** với ASG

▼ 🔗 9. Nexon Internal Patterns

Common Architecture at Nexon[7][9]

```
Internet → Route53 → INFACE Gateway → ALB → EKS Ingress Controller → Pods
```

Alternative for internal:

```
VPC → Internal NLB/ALB → Nginx Ingress Controller → Services
```

NLB + AWS Shield Advanced[3][10]

Use Case: CloudFront replacement cho DDoS protection

- Public NLB với Elastic IP
- AWS Shield Advanced subscription
- Envoy filters + custom metrics

📖 References

AWS Official:

- ELB Best Practices Guide

- ALB User Guide
- NLB User Guide