SYSTEM DESIGN

Basic Networking

Load Balancer , Firewall , CDN

Load Balancer – (লোড ব্যালেন্সার)

Load Balancer কী?

Load Balancer হলো এমন একটি সিস্টেম/ডিভাইস/সফটওয়্যার যা বহু সার্ভারে incoming request সমানভাবে ভাগ করে দেয়, যেন কোনো একটি সার্ভার অতিরিক্ত চাপ না পায়। এর মূল কাজ হলো:

"একাধিক সার্ভারের উপর লোড বিতরণ করা, যেন system দ্রুত ও নিরবিচারে কাজ করে।"

Load Balancer কিভাবে কাজ করে?

- Client → Request পাঠায় Load Balancer এ
- Load Balancer দেখে কোন সার্ভার Healthy এবং কম ব্যস্ত
- সেই সার্ভারে Request পাঠিয়ে দেয়
- Response আসে Load Balancer হয়ে Client-এর কাছে

Load Balancer এর ধরন (OSI Model অনুযায়ী)

ধরণ	স্তর (Layer)	কাজ
L4 Load Balancer	Transport Layer (TCP/UDP)	IP/Port দেখে রিকোয়েস্ট ভাগ করে
L7 Load Balancer	Application Layer (HTTP/HTTPS)	URL, Cookie, Header দেখে decision নেয়

LOAD BALANCER এর SYSTEM DESIGN-এ ভূমিকা

Scalability:

- User বাড়লে, নতুন সার্ভার যুক্ত করে traffic ভাগ করা যায়

-> Fault Tolerance:

- এক বা একাধিক সার্ভার ডাউন হলেও অন্য healthy সার্ভার চালিয়ে যায়

-> High Availability:

- Uptime বাড়ায়, কারণ failover করা যায় দ্রুত

-> SSL Termination:

- HTTPS request Load Balancer-এ ডিকোড হয়, পেছনে HTTP চলে (performance বাড়ে)

বাস্তব উদাহরণ (TEXT DIAGRAM):

```
[Client Request]
       |
   Load Balancer
   /     |     \
Server A  Server B  Server C
```

REAL-WORLD TOOLS

Tool / Provider	ধরন
Nginx	Software Load Balancer (L7)
HAProxy	TCP/HTTP Load Balancer
AWS ELB	Managed Load Balancer
Cloudflare Load Balancer	DNS-based Global Load Balancing
Kubernetes Ingress / Service	Container-level Load Balancing

CDN (CONTENT DELIVERY NETWORK)

CDN কী?
CDN হলো এমন একটি ডিস্ট্রিবিউটেড সার্ভার নেটওয়ার্ক, যা ওয়েবসাইটের স্ট্যাটিক এবং কখনও কখনও ডায়নামিক কনটেন্ট ব্যবহারকারীর কাছাকাছি অবস্থান করা সার্ভার থেকে সরবরাহ করে।

ফলাফল: লোড টাইম কমে যায়, সার্ভার লোড কমে, এবং ভালো ইউজার এক্সপেরিয়েন্স পাওয়া যায়।

CDN কিভাবে কাজ করে?

- ইউজার ওয়েবসাইট বা অ্যাপ থেকে রিকোয়েস্ট পাঠায়
- CDN নিকটস্থ EDGE SERVER খুঁজে নেয়
- যদি EDGE SERVER-এ CACHED কনটেন্ট থাকে → ওখান থেকে সরাসরি ভিজিটর কে দেয়
- যদি না থাকলে মূল ORIGIN SERVER থেকে কনটেন্ট নিয়ে EDGE SERVER-এ ক্যাশ করে ইউজারকে দেয়

CDN এর প্রধান উপাদানসমূহ

উপাদান	কাজ
Edge Servers	বিশ্বজুড়ে ছড়িয়ে থাকা সার্ভার
Origin Server	মূল ওয়েবসাইট/অ্যাপের সার্ভার
PoPs (Points of Presence)	সার্ভারের ফিজিক্যাল লোকেশন গুলো
Caching	কনটেন্ট সংরক্ষণ করে রাখা

CDN এর সুবিধা :

1. এটি নিকটবর্তী সার্ভার থেকে ডেটা দেয়ার ফলে দ্রুত লোড হয়
2. মূল সার্ভারে কম লোড পড়ে, কারণ cached content দিয়ে দেয়
3. যদি সার্ভার ডাউন হলেও অন্য সার্ভার সার্ভিস দেয়
4. বেশিরভাগ CDN DDoS আক্রমণ ফিল্টার করে থাকে

CDN এর System Design এ ভূমিকা :

- Static Asset যেমন ছবি, CSS, JS, ভিডিও , সার্ভ করে থাকে
- Dynamic Content এর কিছু অংশ caching (যেমন API response) সার্ভ করে
- Global Scaling সহজ হয়
- সার্ভার লোড কমিয়ে দেয়
- ইউজার ইন্টারঅ্যাকশন দ্রুত হয় (UX উন্নত হয়)

CDN Cache Control ও TTL:

- HTTP Header-এ Cache-Control দিয়ে নির্ধারণ করা হয় কতক্ষণ কনটেন্ট ক্যাশে থাকবে
- TTL (Time To Live) মানে cache-এ রাখা সময়কাল
- TTL (Time To Live) মানে cache-এ রাখা সময়কাল

জনপ্রিয় CDN সেবা প্রদানকারীর কোনগুলো চলুন দেখে নেই :

CDN Provider	বিশেষত্ব
Cloudflare	Security & Performance focus
Akamai	Largest global footprint
AWS CloudFront	Deeply integrated with AWS
Fastly	Real-time CDN with instant purging
Google Cloud CDN	Google infra এর উপর ভিত্তি করে

CDN Architecture (Text Diagram)

```
[User Request]
      ↓
[Nearest CDN Edge Server]
      ↓ (If cache miss)
[Origin Server]
      ↓
[CDN caches response]
      ↓
[User gets response fast]
```

LEARN HUNTER

FIREWALL & SECURITY

Firewall কী?

Firewall হলো একটি নিরাপত্তা ব্যবস্থা, যা নেটওয়ার্কে ঢোকার ও বের হওয়ার ডেটা প্যাকেটগুলোকে নিয়ন্ত্রণ করে। এটা নিয়ম (rules) অনুযায়ী নির্ধারণ করে কোন ট্রাফিক যেতে পারবে, আর কোনটা বন্ধ থাকবে।

Firewall এর ধরন :

ধরন	কাজ
Network Firewall	Router বা Dedicated Device হিসেবে কাজ করে, পুরো নেটওয়ার্কে প্রটেকশন দেয়
Host-based Firewall	সার্ভারের ভিতরে সফটওয়্যার হিসেবে থাকে, ওই সার্ভারকে প্রটেক্ট করে
Web Application Firewall (WAF)	ওয়েব অ্যাপের HTTP ট্রাফিক ফিল্টার করে SQL Injection, XSS থেকে সুরক্ষা দেয়

FIREWALL এর কাজ

1. Port ও IP ঠিকানা ব্লক/অ্যালাউ করে দেয়
2. ট্রাফিক ফিল্টারিং (inbound & outbound) করে
3. প্রোটোকল নিয়ন্ত্রণ (TCP, UDP, ICMP) করে
4. লগিং ও মনিটরিং করে

Firewall Rules উদাহরণ

Rule Number	Action	Protocol	Source IP	Destination Port
1	Allow	TCP	Any	80 (HTTP)
2	Allow	TCP	Any	443 (HTTPS)
3	Deny	All	Any	All

SYSTEM DESIGN এ FIREWALL এর গুরুত্ব

1. Unauthorized Access বন্ধ করা
2. DDoS আক্রমণ থেকে প্রটেকশন করা
3. Internal network segmentation
4. Compliance ও Security Policy রক্ষা করা

WEB APPLICATION FIREWALL (WAF)

1. ওয়েব অ্যাপের জন্য বিশেষ Firewall এটি
2. SQL Injection, Cross-site scripting (XSS) ইত্যাদি আক্রমণ আটকায়
3. Cloudflare, AWS WAF, ModSecurity এর মতো টুলস ব্যবহার হয়

SECURITY GROUPS (CLOUD ENVIRONMENT)

1. AWS, Azure, GCP এ Security Group ব্যবহার হয় Firewall এর মতো
2. নির্দিষ্ট IP ও Port গুলোকে অনুমতি দেয়
3. Stateless বা Stateful হতে পারে

NETWORK SECURITY BEST PRACTICES

1. Minimum privilege (প্রয়োজনীয় শুধু অনুমতি দেয়া)
2. Regular audit & monitoring
3. Patch & Update firewall rules
4. Use VPN / Private Network for sensitive communication

LEARN HUNTER

শেষ কথা:

সুতরাং এই ছিল আজকের ছোট আলোচনা আমরা Load Balancer , CDN এবং Firewall খুব ভালো করে জানলাম এগুলো কি? কেন দরকার উপকারিতা গুলো কি কি। পরবর্তীতে আমরা CAP Theorem নিয়ে আলোচনা করবো সাথেই থাকুন

LEARN HUNTER