Web Application Security & Optimization

Praktisi Mengajar - Politeknik Hasnur
me@adityaputra.com

Typical components of web applications

- Domain
- Hosting
- Application
    - Backend: PHP, java, nodeJS, Python, golang, etc.
    - Frontend: HTML, CSS, JS
    - Data storage: Database, file storage, etc.

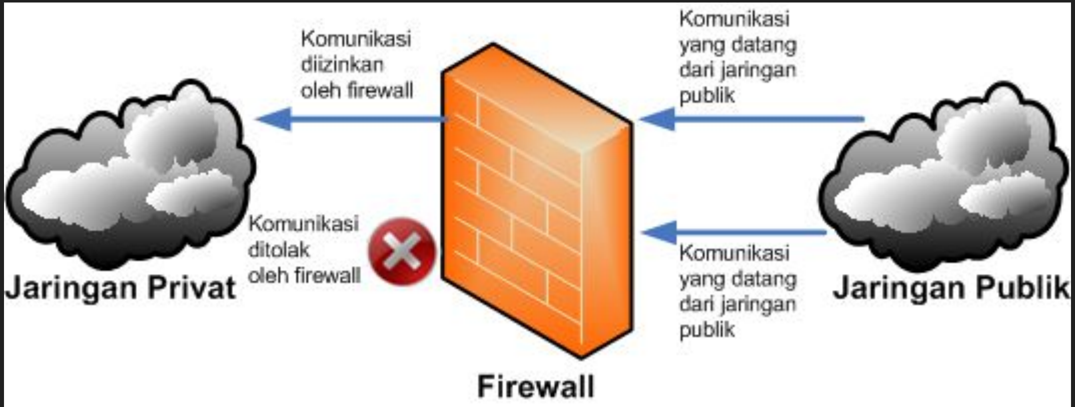
Problem is…

- Web applications need to be **secure**
- Web applications need to be **fast**
- Web applications need to be **highly available**
- Web applications need to be **scalable**
- Web applications need to be **cost-efficient**

Securing web applications

- Use strong passwords / key, enable two-factor-authentication everywhere
- Follow developer's recommendation for best security practices
  - Check their documentation
    - https://wordpress.org/support/article/hardening-wordpress/
    - https://docs.magento.com/user-guide/v2.3/magento/magento-security-best-practices.html
- GIve least access to those who needs (developers, APIs, etc.)
  - Only allow specific ports to only specific IP address
  - Create separate user accounts for each specific needs
  - Never allow public access except you really have to
- Put firewall in multiple places

Firewalls

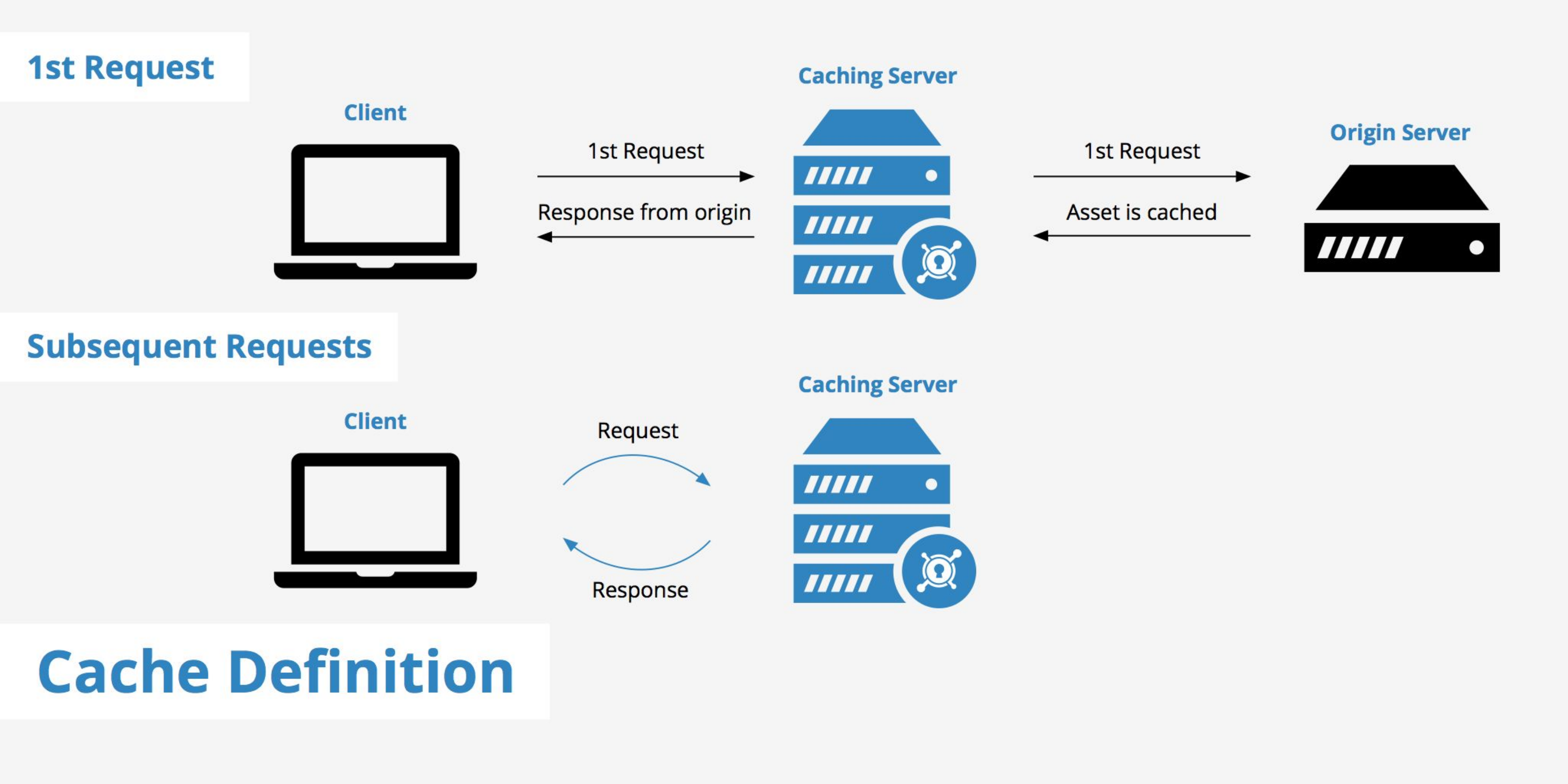

Komunikasi diizinkan oleh firewall
Komunikasi yang datang dari jaringan publik
Komunikasi ditolak oleh firewall
Komunikasi yang datang dari jaringan publik
Jaringan Privat
Jaringan Publik
Firewall

- OS firewall
- Cloud / VPS firewall
- Proxy: cloudflare, akamai, fastly, etc.

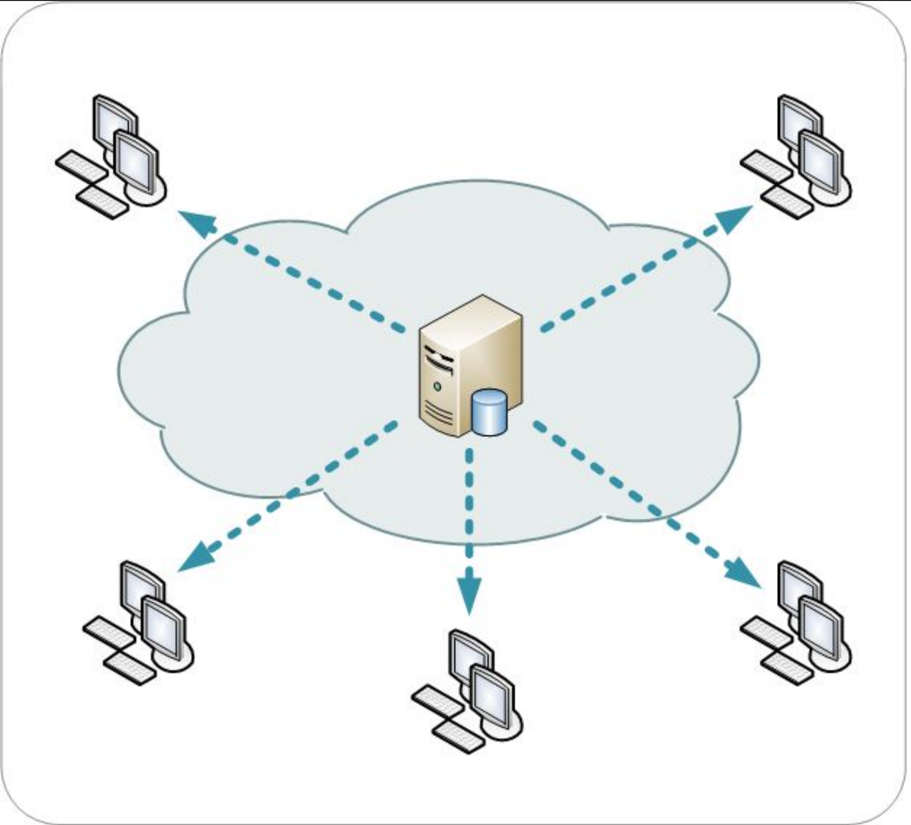
Building fast website

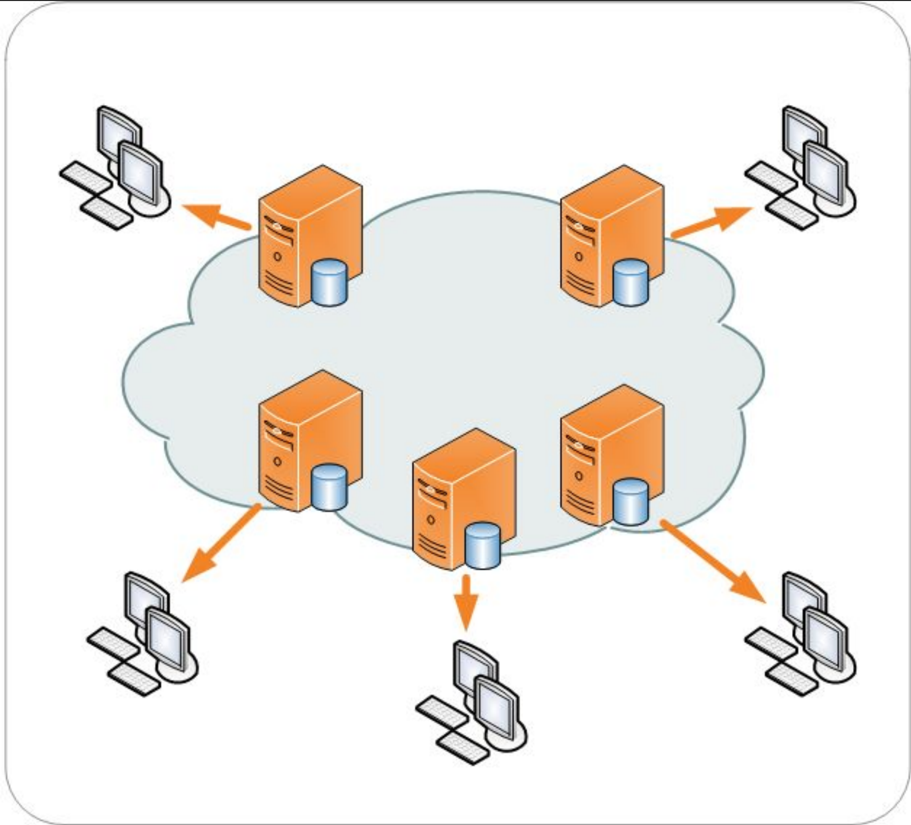
- Fast website loads in milliseconds
- Aspects to consider:
  - Application itself
  - Server specification
  - Network
  - **Caching & CDN**

Cache


1st Request
Client
1st Request
Response from origin
Caching Server
1st Request
Asset is cached
Origin Server
Subsequent Requests
Client
Request
Response
Caching Server
Cache Definition

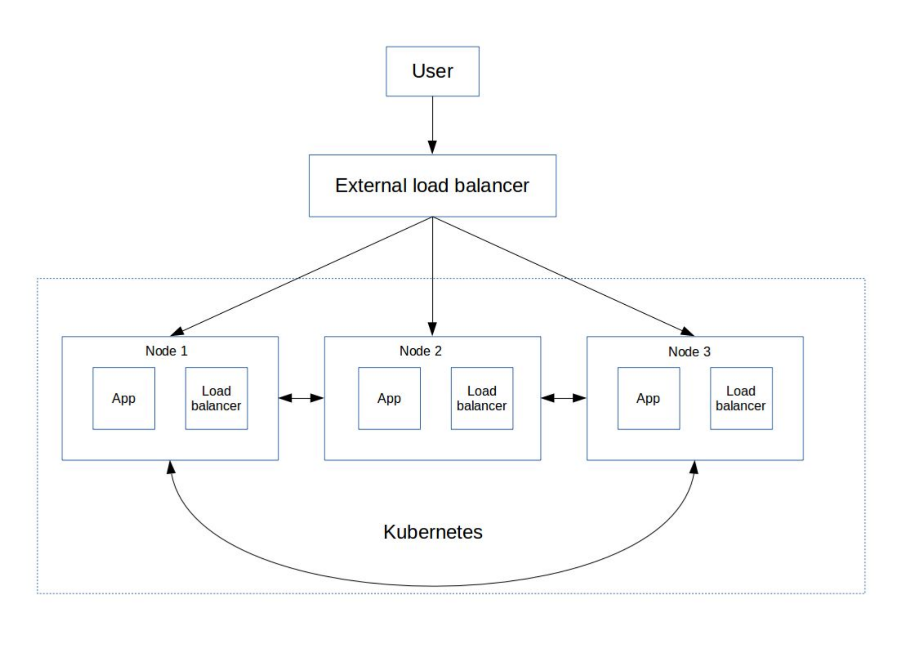
CDN





Building highly-available & scalable application

- HA application: application that is designed to have higher availability than average application
- How to achieve:
  - Multi server app
  - Load balancer
  - Kubernetes
  - Docker
  - Cloud



Cost efficiency

- Cost is a major aspect to consider
- Tools to use:
    - CDN
    - Varnish / cache
    - On-demand pricing strategy VS reserved instances

Group Assignments

Implementasikan HTML & CSS sesuai desain yang telah diusulkan, kemudian upload ke web hosting (sama seperti pertemuan sebelumnya)