**LOMBA KOMPETENSI SISWA**
**SEKOLAH MENENGAH KEJURUAN**
**TINGKAT PROVINSI JAWA TIMUR TAHUN 2023**

# IT NETWORK SYSTEMS ADMINISTRATION


Test Project

# MODUL A – CLIENT SERVER ENVIRONMENT

## Description

A branch of a big company has hired you to configure their newly built infrastructure. There will be five sites, DMZ, Internal, Inner, Outer, and External. They will use both Windows and Linux for their services. Refer to the logical topology for the visualization of the new branch infrastructure.

### Credentials

- Debian Server
  username : root
  password : Skills39

- Windows 10
  username : competitor
  password : Skills39

- Windows Server
  username : Administrator
  password : Skills39

# General Configuration

## Basic Configuration

- Configure all servers with hostname and IP Address according to Appendix.
- Configure all linux servers to allow non-root login via SSH.
- Configure all windows servers to be pingable.

## Persistent Configuration

- Make sure all configuration persistent across reboot. All VMs will be rebooted before marking begin.

# Supporting Services

## DHCP and Network Booting

- **FIREWALL** will serve as both DHCP Server and TFTP Server. You can freely use any tools to provide the service.
  - Configure TFTP server at **FIREWALL** to provide boot images for debian OS.
  - Configure **FIREWALL** to serve DHCP server that supports PXE boot using TFTP from previous task.
  - Configure DHCP to allow only 'internal' to do PXE booting.
- We will use **Office VM** to test the network boot.
- Enable DHCP Relay in **EDGE1** and **EDGE2** to forward DHCP requests to **FIREWALL**.
- Configure DHCP to provide addresses to DMZ zone. Use static mapping for all servers according to **appendix table**.
- Configure DHCP to provide addresses to Internal zone. Use available unused IP ranges in the subnet, refer to **appendix table**.

## Firewall and Traffic Logging

- Configure **FIREWALL** using iptables LOG module, log following traffics:
  - Log outgoing traffic coming from this server's DHCP port to Internal zone.
  - Log outgoing traffic coming from this server's TFTP port to anywhere.
  - Log incoming HTTPS traffic.
  - Put all logs in default location (/var/log/syslog)
- Create simple firewall rule in **EDGE1** and **EDGE2** to block these traffic:
  - From **FIREWALL** to **SERVICE** via HTTP and HTTPS port.

## Routing and NAT

- Enable routing in **FIREWALL**, **EDGE1** and **EDGE2**.
- Enable port NAT in **FIREWALL** to allow **EDGE1**, **EDGE2**, and Internal Servers to reach public network.
- Route traffic from Internal to **FIREWALL**, and vice-versa via **EDGE1** and/or **EDGE2**
  - Enable routing failover if one of the servers is down.
    - Use this IP as Virtual IP to be used as gateway: 172.16.233.124/25
  - Do not route traffic from the public network.
- Route traffic from **DMZ** to **FIREWALL**, and vice-versa via **EDGE1** and/or **EDGE2**
  - Enable routing failover if one of the servers is down.
    - Use this IP as Virtual IP to be used as gateway: 172.16.234.252/24
  - Do not route traffic from the public network.

## Certificate Authority

- Configure **STORAGE** as Root CA.
  - Use Common Name: LKS2023-Root
  - Approve Intermediate CA Requests for MAIL.
  - Save Intermediate CA certificate files without the key in directory /backup/ca in **MAIL** server.
- Configure **MAIL** as Intermediate CA Issuer.
  - Use Common Name: LKS2023-Intermediate
  - In this Intermediate CA, issue the certificates required for other services.
  - For record, place all generated certificates in /backup/certs in **MAIL** server.

## Server Configuration

- Install sudo in **STORAGE** and only allow user ‘ops’ to use sudo. Make sure all other users are not able to use sudo.
  - Create the user ‘ops’ with password Skills39

# Core Services

## Email

- Configure **MAIL** as a centralized mail server using any application that supports SMTP and IMAP using negotiable TLS.
  - Use the domain itnsa.id so mail can be sent directly to @itnsa.id mail address.
  - Configure SMTP to listen in port 25.
  - Enable negotiable TLS using certificate from Corporate CA.
  - Configure IMAP to listen in port 143
  - Enable negotiable TLS using certificate from Corporate CA.
- Enable web-based email using roundcube.
  - Enable https access using certificate from Corporate CA.
  - Make it accessible with the domain webmail.itnsa.id
- Configure **Mail** Users according to table in the appendix
- Configure **Mail** Groups notification@itnsa.id with following members:
  - ops@itnsa.id
  - dev@itnsa.id

## VPN and Virtual Users

- Configure LDAP in **MAIL** to provide users available for VPN Authentication.
  - Configure using domain dc=itnsa,dc=id.
  - Create user ‘vpn’ with password ‘Skills39’ for VPN testing.
- Configure openvpn in **MAIL** to provide remote access VPN to remote clients.
  - Allow any client to connect using username and password authentication via LDAP.
  - Configure remote clients to use following IP:
    - Start: 10.20.22.10
    - End: 10.22.22.50
    - Subnet: 255.255.255.0
    - Gateway: 10.22.22.1
- You can use **FIREWALL** to test the VPN Client connection, but make sure to disconnect after testing.
  - Distribute client configuration file to connect to **FIREWALL** in /etc/openvpn/client.ovpn

## Main Website

- Use **SERVICE** to hosts all department's website:
  - managers.itnsa.id at C:\web\managers
  - dev.itnsa.id at C:\web\dev
  - 10 ops website:
    - ops01.itnsa.id at C:\web\ops01
    - ops02.itnsa.id at C:\web\ops02
    - ops03.itnsa.id at C:\web\ops03
    - …
    - ops09.itnsa.id at C:\web\ops09
    - ops10.itnsa.id at C:\web\ops10
- Enable basic authentication for managers.itnsa.id, allow user 'manager' with password 'Skills39'
- Enable HTTPS for managers.itnsa.id and dev.itnsa.id.
  - Use Certificate from Intermediate CA that points to wildcard domain of *.itnsa.id.
- Refer to the **appendix** for website content.
- Make sure the DNS record is also created at Main DNS.

## Main DNS

- Configure **SERVICE** to serve DNS for all itnsa.id domains.
  - Add all servers hostname to be accessible via {hostname}.itnsa.id
    - The subdomain points to all available IP addresses of the servers according to the appendix.
  - Refer to other tasks for required records, including but not limited to:
    - Email
    - All Web Domains
  - Set NS record for the domain to **SERVICE**.

## Backup and Shared Folder

- Configure **STORAGE** to host a CIFS shared folder that can be mounted at Windows Server.
  - Use samba or any other similar application.
  - Use Directory: /share
  - Allow all anonymous to read and write to the directory.
- Create a backup job using the windows server backup feature.
  - Backup C:\web in **SERVICE** to the shared folder daily at any hour.
  - Make sure the backup is successfully executed at least once.

# Appendix

## IP Address Table

| Hostname | Operating System | Service | IP Address | Preinstalled |
|---|---|---|---|---|
| EDGE1 | Windows Server 2019 desktop | • Load Balancing Traffic<br>• Routing<br>• Routing Failover | 172.16.234.253/24<br>172.16.233.125/25<br>172.19.99.252/28 | yes |
| EDGE2 | Windows Server 2019 desktop | • Load Balancing Traffic<br>• Routing<br>• Routing Failover | 172.16.234.254/24<br>172.16.233.126/25<br>172.19.99.253/28 | yes |
| SERVICE | Windows Server 2019 desktop | • DNS<br>• Web Service<br>• Backup and Restore | 172.16.233.11/25 | yes |
| FIREWALL | Debian 11 Server | • FIREWALL (iptables)<br>• Routing<br>• Network Boot<br>• DHCP | 172.19.99.254/28<br>172.12.33.25/30 | yes |
| REMOTE | Windows 10 | • VPN Client | 172.16.233.10/25<br>172.12.33.26/30 | yes |
| MAIL | Debian 11 Server | • Certificate Authority<br>• LDAP<br>• Mail Service<br>• Remote Access VPN (openvpn) | 172.16.234.21/24 | yes |
| STORAGE | Debian 11 Server | • Certificate Authority<br>• Role Based Access Policy<br>• Shared File Service | 172.16.233.15/25 | yes |
| OFFICE | None | • Network Boot Test | DHCP | no |

## Mail Users

| Email | Password | Group |
|---|---|---|
| ops@itnsa.id | Skills39 | notification@itnsa.id |
| dev@itnsa.id | Skills39 | notification@itnsa.id |
| admin@itnsa.id | Skills39 | - |

## Website Content

### managers.itnsa.id

```
<h1> managers.itnsa.id </h1>
This website is managed by admin@itnsa.id
```

### dev.itnsa.id

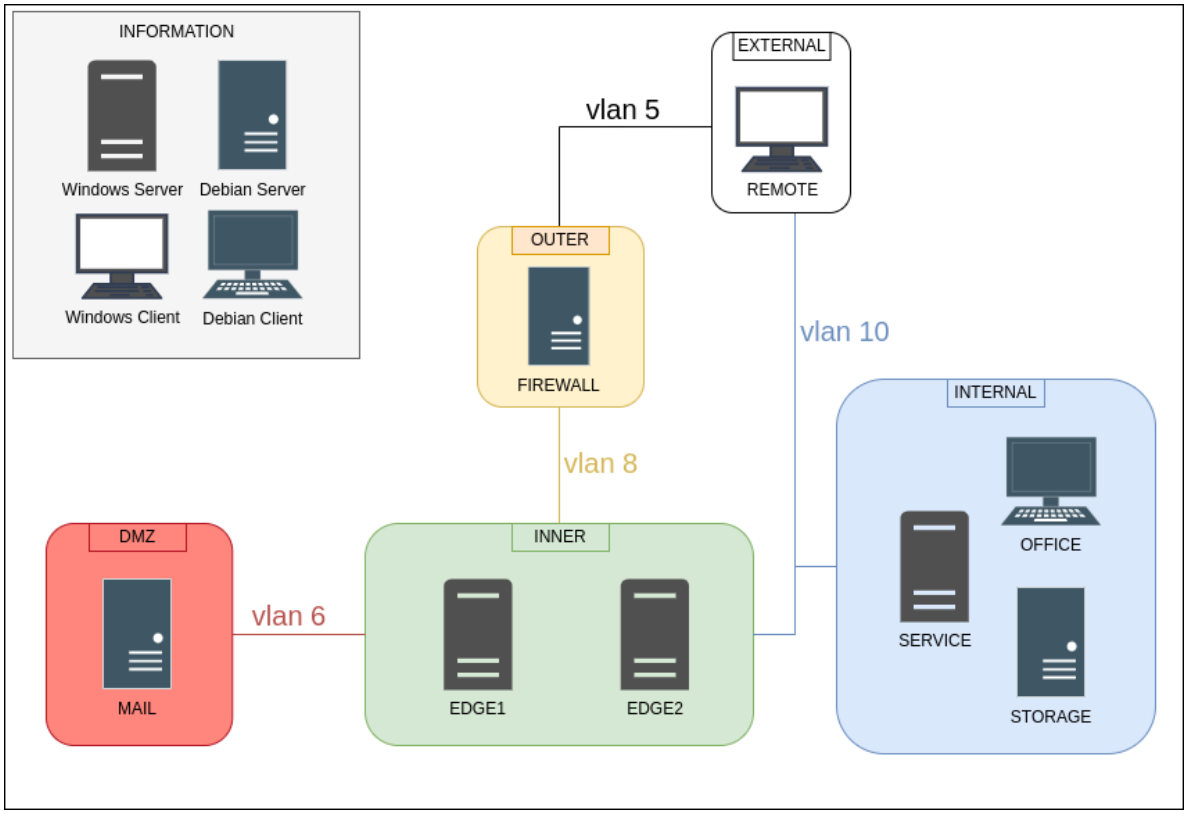
```
<h1> dev.itnsa.id </h1>
This website is managed by dev@itnsa.id
```

### opsXX.itnsa.id

- Replace XX in file content with user number, for example ops01.itnsa.id

```
<h1> opsXX.itnsa.id </h1>
This website is managed by ops@itnsa.id
```

## Topology


INFORMATION
Windows Server
Debian Server
Windows Client
Debian Client
EXTERNAL
REMOTE
vlan 5
OUTER
FIREWALL
vlan 10
INTERNAL
OFFICE
SERVICE
STORAGE
vlan 8
DMZ
MAIL
vlan 6
INNER
EDGE1
EDGE2