Balai Pengembangan Talenta Indonesia
Kementerian Pendidikan Dasar dan Menengah

KEMENDIKDASMEN RAMAH #PENDIDIKAN BERMUTU UNTUK SEMUA

TEST PROJECT

LKS DIKMEN
TINGKAT NASIONAL

LOMBA KOMPETENSI SISWA DIKMEN 2025

SMK/SMA/MAK/MA

Cabang Ajang

Teknologi Informasi Sistem Administrasi Jaringan

(IT Network System Administration)

ACTUAL TEST PROJECT
MODUL A – LINUX ENVIRONMENT

IT NETWORK SYSTEMS ADMINISTRATION

LOMBA KOMPETENSI SISWA DIKMEN
TINGKAT NASIONAL 2025

Introduction

This Linux Environment project is a practice setup to help you learn how to build and manage a secure computer network using Debian 12. You will configure different servers for specific roles: the internal server handles DNS, user login (LDAP), and digital certificates; the DMZ servers provide email and website services that can be accessed from the internet; the firewall server controls what traffic is allowed in and out, and also sets up a secure VPN connection; and the client computer is used to test everything—like checking if websites and email are working properly through the VPN. This project helps you understand how real companies manage and protect their networks.

Login

Username: root/user

Password: Skills39!

System Configuration

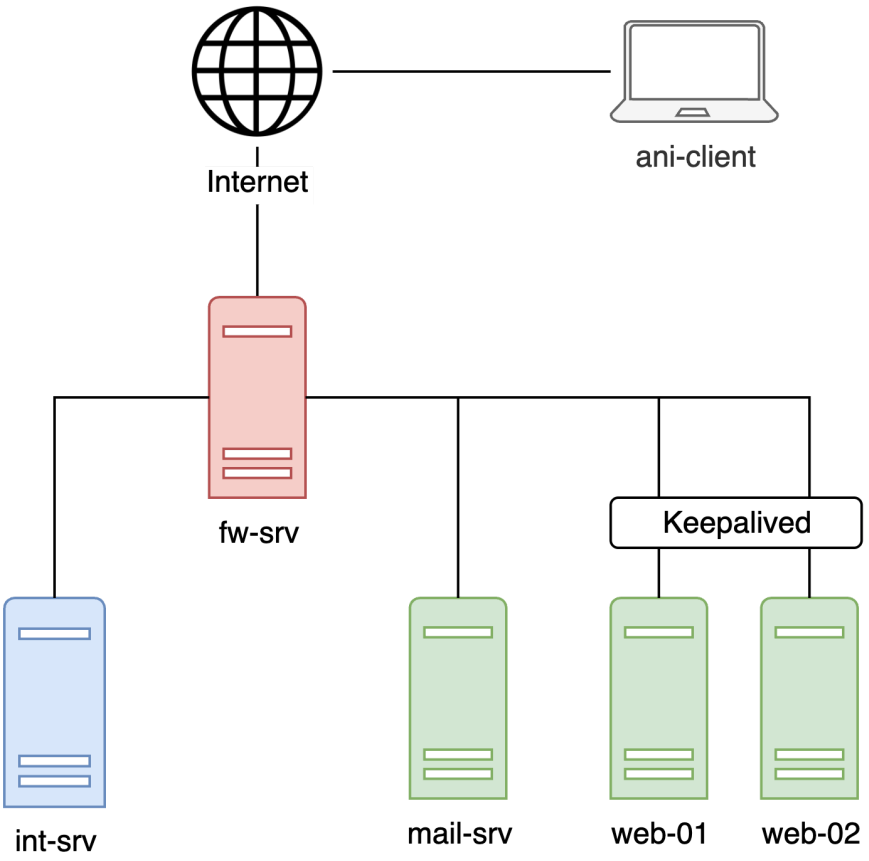
Timezone: Asia/Jakarta

General Configuration

Fully Qualified Domain Name	Ipv4	Services
fw.lksn2025.id	internet: 100.100.100.200/24 int-zone: 192.168.1.254/24 dmz-zone: 172.16.1.254/24 mgmt: 10.0.0.11/24	Firewall(nftables), VPN Server(OpenVPN)
int-srv.lksn2025.id	int-zone: 192.168.1.10/24 mgmt: 10.0.0.10/24	DNS Server(Bind9), LDAP Directory(slapd), Certificate Authority(OpenSSL)
mail-srv.lksn2025.id	dmz-zone: 172.16.1.10/24 mgmt: 10.0.0.12/24	Mail Server (Postfix(SMTP), Dovecot(IMAP)), Webmail(Roundcube)
web-01.lksn2025.id	dmz-zone: 172.16.1.21/24 mgmt: 10.0.0.13/24	Virtual IP(keepalived), HAProxy, Web Server
web-02.lksn2025.id	dmz-zone: 172.16.1.22/24 mgmt: 10.0.0.14/24	Virtual IP(Keepalived), Load Balancer(Haproxy), Web Server(Nginx)
ani-clt.lksn2025.id	internet: 100.100.100.100/32 mgmt: 10.0.0.15/24	Client

NAME	NETWORK
int-zone	192.168.1.0/24
dmz-zone	172.16.1.0/24
internet	100.100.100.0/24
vpn	10.10.0.0/24
mgmt	10.0.0.0/24

Topology



Networking

To make your life a bit easier, networking has been preconfigured on all machines.

Notes

- On the ani-client machine, ZealDocs is already installed for accessing documentation related to Ansible, Bash, and Python. Visual Studio Code (VSCode) is also installed.
- Ensure that your configuration is saved persistently—any changes must remain intact after a server reboot.
- For the assessment process, the system depends on the SSH service. Therefore, do not modify the SSH configuration under any circumstances!

Part 1 INT (Internal)

The internal server int-srv.lksn2025.id is responsible for providing core infrastructure services, including DNS, LDAP authentication, and certificate authority (CA) functions. This setup ensures centralized user management and secure communication across the network.

int-srv.lksn2025.id

DNS

Set up a DNS server using BIND9 to manage domain names.

1. Install & Configure BIND9
2. Create DNS Zones
   - Create a forward zone for: lksn2025.id
   - Create a reverse zone for the int-zone and dmz-zone
3. Add DNS Records
   - Add forward and reverse records for all servers listed in the general configuration.
   - Add additional records on the table.

Type	Name	Value/Target
A	www	100.100.100.200
A	mail	172.16.1.10
A	vip	172.16.1.100
A	vpn	100.100.100.200
CNAME	www.int	vip.lksn2025.id
MX	@	10 mail.lksn2025.id

LDAP

Install and configure LDAP using slapd to manage user accounts. These users will be used to log in to the mail server.

1. Install LDAP and use slapd
2. Create LDAP users
   - Create the following users in LDAP. These users will be used for email login (authentication)

Full Name	Username (uid)	Password	Organizational Unit (OU)	Email Address
Administrator	admin	Skills39	-	-
Ani Utami	ani	Skills39	mail,vpn	ani@lksn2025.id
kyw1 kyw2 … kyw5	kyw1 kyw2 … kyw5	Skills39	mail	kyw1@lksn2025.id kyw2@lksn2025.id … kyw5@lksn2025.id
vpn1 vpn2 vpn3	vpn1 vpn2 vpn3	Skills39	vpn	-

CA

Use OpenSSL to create your own Certificate Authority (CA) and generate certificates for your server (web and mail).

1. Create Root CA
   - Make a Root CA with the common name: “LKSN2025-CA”
   - Add fields:
     - C = ID
     - ST= Jakarta
     - O = ITNSA
   - Add attributes
     X509v3 Key Usage: critical
     Certificate Sign
     X509v3 Basic Constraints: critical
     CA:TRUE
   - Install LKSN2025-CA on every server and client
2. Create Certificates for Servers
   - Generate and sign the following certificates directly using the Root CA:
   - A certificate for web server, valid for: www.lksn2025.id, www.int.lksn2025.id
   - A certificate for mail server, valid for mail.lksn2025.id
   - A certificate for vpn server has extended Key Usage serverAuth
3. Save All Certificates
   - Save the certificates in this folder: /opt/grading/ca
     - ca.pem: Root CA certificate
     - web.pem: Web server certificate
     - mail.pem: Mail server certificate
     - vpn.pem: OpenVPN server certificate

Ansible

We will set up Ansible on the server int-srv and make it control server web-02. All Ansible files (settings, playbooks, and modules) must be saved in the /etc/ansible directory.

1. Configure the Ansible inventory to include web-02, so you can test the connection using the following command:
   ansible web-02 -m ping
2. Create playbook 01-web-int.yml
   - This playbook will install Nginx
   - It will also create a virtual host that listens on port 8081
   - When you open the website, it will show the message: “This is web internal”
   - Make the playbook idempotent
   - To run the playbook, use this command:
     ansible-playbook /etc/ansible/01-web-int.yml

Part 2 DMZ (Demilitarized Zones)

The DMZ zone hosts public-facing services such as the mail server and high-availability web servers. These servers are isolated from internal systems but must securely communicate with them for functions like LDAP authentication and certificate verification.

mail.lksn2025.id

Mail Server

Deploy a fully functional mail server using Postfix and Dovecot to allow users to send and receive emails under the domain lksn2025.id.

1. Software Installation
   - Postfix - to manage sending and receiving emails SMTP.
   - Dovecot - to enable users to access and read emails via IMAP.
2. Mail Server Configuration
   - Configure the server to handle mail delivery for the domain lksn2025.id
   - Users should be able to read their emails using IMAP
   - Enforce TLS encryption for all connections between email clients and the server
     - If the Certificate Authority (CA) task has been completed, use the certificate issued for the mail server.
     - If not, generate a self-signed certificate.
   - Ensure clients that trust the LKSN2025-CA can validate the certificate.
3. LDAP Integration
   - Integrate with LDAP to authenticate users via int-srv.lksn2025.id.
   - Set up Maildir directories for the following users:
     - ani
     - kyw1 through kyw5
   - Ensure that the LDAP user ani can
     - Login in using ther UID (username).
   - Test: use mailutils to confirm that user ani can send an email to themselves.
   - Restrict login access:
     - Only users under ou=mail are permitted to authenticate and use the mail server.
4. Webmail Access
   - Install Roundcube using Apache2 as the web server
   - Expose the Roundcube webmail interface on:
     - http://mail.lksn2025.id

web-01.lksn2025.id & web-02.lksn2025.id

HA Web

Set up a high-availability reverse proxy system using HAProxy and Keepalived on two servers: web-01 and web-02.

1. Keepalived Configuration (Virtual IP)
    - Create a virtual IP (172.16.1.100/24) that will automatically move to the backup server if the main server goes down.
    - web-01: acts as the MASTER with priority 110
    - web-02: acts as the BACKUP with priority 100
2. HAProxy Configuration for Load Balancing
    - Install and configure HAProxy on both servers (web-01 and web-02) to distribute traffic to two Nginx web servers:
        - web-01: 172.16.1.21:8080
        - web-02: 172.16.1.22:8080
    - All HTTP requests must be redirected to HTTPS.
    - HAProxy should perform TLS termination (HAProxy handles HTTPS and forwards to Nginx using HTTP).
    - Add an HTTP header via-proxy: hostname to responses (replace “hostname” with the proxy’s hostname) to help with troubleshooting.
    - If you already have a certificate from your CA, use the web certificate (web.pem).
        - Make sure a client that only trusts your root CA can validate the entire certificate chain.
        - If not, create a self-signed certificate.
3. Web Server nginx
    - On web-01 and web-02 install nginx and listen port 8080 with index.html “Hello from ${hostname}”

Part 3 Firewall

The firewall server fw.lksn2025.id acts as a secure gateway for internal and DMZ networks. It is responsible for controlling traffic flow, providing internet access, forwarding services, and securing VPN connectivity.

fw.lksn2025.id

nftables

Create firewall and NAT rules using nftables to control which traffic is allowed or blocked in your network.

1. Allow Internet Access
   - Devices in the INT (internal) and DMZ networks can access the internet.
2. NAT Masquerade
   - When sending traffic from your network to the internet (through the WAN), the firewall must replace the source IP with its own WAN IP using masquerade NAT.
3. Port Forwarding
   - Forward incoming traffic from the internet to servers in the DMZ:

Port	Protocol	Forward To
80	TCP	172.16.1.100
443	TCP	172.16.1.100
53	TCP/UDP	192.168.1.10

4. VPN Access
   - VPN clients should be able to reach both internal and DMZ networks.
5. Mail Server to LDAP
   - The mail server must be allowed to query the LDAP service running on int-srv01.
6. Block Everything Else
   - Any other traffic that's not mentioned above should be blocked (default deny).

OpenVPN

Ensures secure access to internal web applications, email systems, and internal DNS services.

- Install OpenVPN along with the LDAP authentication plugin
- Set up a Tun interface for Layer 3 tunneling:
  - Interface type: tun
  - Uses UDP protocol on port 1194
  - Assigns VPN clients to the 10.10.10.0/24 subnet
- Utilize a certificate issued by LKSN2025-CA
- Enable LDAP-based authentication via int-srv.lksn2025.id
  - Authentication base DN: ou=vpn,dc=lksn2025,dc=id

Part 4 Client

The client machine ani-client.lksn2025.id represents a remote workstation that connects securely to internal and DMZ services through VPN. It is used to validate the overall infrastructure by testing access to web, DNS, and email services.

General Configuration

1. Create a local user named ani (Ani Utami)
   - Set the password to Skills39
   - Grant ani passwordless sudo privileges
2. Set up the OpenVPN client
   - Save the .ovpn configuration file to /etc/openvpn/client/lksn2025.conf
   - Create a file /etc/openvpn/auth.txt to securely store OpenVPN credentials. use user ani ldap ou=vpn,dc=lksn2025,dc=id
   - Create a systemd service named openvpn-client.service to enable automatic startup on boot and ensure persistent VPN connectivity
3. Ensure access to internal web services via vpn
   - Able to access https://www.lksn2025.id and https://www.int.lksn2025.id without certificate errors when connected to the VPN
4. Verify webmail access through VPN
   - Access Roundcube webmail at https://mail.lksn2025.id after VPN connection
   - Successfully log in using the account ani@lksn2025.id
   - Able to send an email to the same account (self-mail test) without issue