LOMBA KOMPETENSI SISWA
PENDIDIKAN MENENGAH

TINGKAT PROVINSI
TAHUN 2025

IT NETWORK SYSTEMS ADMINISTRATION
ADMINISTRATION DES SYSTÈMES ET DES RÉSEAUX
Main Skill Sponsor – Sponsor principal du métier
CFA

TEST PROJECT
MODUL A – LINUX ENVIRONMENT

IT NETWORK SYSTEMS ADMINISTRATION

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.itnsa.id	INT: 10.10.10.254/24, DMZ: 10.10.20.254/24, WAN: 100.100.100.254/24, MGMT: 192.168.2.15/24	VPN (wireguard), firewall (nftables)
int-srv.itnsa.id	INT: 10.10.10.10/24, MGMT: 192.168.2.11/24	DNS Server (bind9), LDAP (slapd), CA (openssl), ansible
mail.itnsa.id	DMZ: 10.10.20.10/24, MGMT: 192.168.2.12/24	Mail Server (postfix + dovecpt)
web-01.itnsa.id	DMZ: 10.10.20.21/24, MGMT: 192.168.2.13/24	Virtual IP(keepalived), HAProxy, Web Server
web-02.itnsa.id	DMZ: 10.10.20.22/24, MGMT: 192.168.2.14/24	Virtual IP(keepalived), HAProxy, Web Server
budi-clt.itnsa.id	WAN: 100.100.100.100/24, MGMT: 192.168.2.16/24	E-mail client, vpn client

Networking

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

Notes

For the assessment process, we use a system that relies on the SSH service. Therefore, you are strictly prohibited from modifying the SSH configuration !!!

Part 1 INT (Internal)

The internal server int-srv.itnsa.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.itnsa.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: itnsa.id
   - Create a reverse zone for the internal IP address range (for example: 10.10..)
3. Add DNS Records
   - Add forward and reverse records for all servers listed in the general configuration.
   - Add additional records to the table.

Type	Name	Value/Target
A	www	100.100.100.254
A	vrrp	10.10.20.100
CNAME	www.int	vrrp.itnsa.id
MX	@	10 mail.itnsa.id

LDAP

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

1. Install LDAP 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!	-	-
Boaz Salossa	boaz	Skills39!	Employees	boaz.salossa@itnsa.id
Budi Sudarsono	budi	Skills39!	Employees	budi.sudarsono@itnsa.id

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 name: “ITNSA Root CA”
   - For other fields like Country, State, etc., you can use any value.

- Add attributes
  X509v3 Key Usage: critical
  Certificate Sign
  X509v3 Basic Constraints: critical
  CA:TRUE
- Install ITNSA Root CA on every servers and clients

2. Create Certificates for Servers
   - Generate and sign the following certificates directly using the Root CA:
   - A certificate for the web server, valid for: www.itnsa.id, www.int.itnsa.id
   - A certificate for the mail server, valid for mail.itnsa.id
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

Ansible

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

1. Create playbook 01-user.yml
   - This playbook will create a new user on the server
   - Set password Skills39!, but for the username, we will use variables, so they can be changed easily
   - Make the playbook idempotent
   - To run the playbook, use this command:

     ```
     ansible-playbook /etc/ansible/01-user.yml -e user_name=developer
     ```
2. Create playbook 02-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/02-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.itnsa.id

Mail Server

Set up a mail server using Postfix and Dovecot so users can send and receive emails for the domain itnsa.id.

1. Install Mail Server Software
   - Postfix (for sending and receiving emails)
   - Dovecot (for letting users read their emails)
2. Mail Server Configuration
   - The mail server must send and receive emails for the domain: itnsa.id
   - Users should be able to read their emails using IMAP
   - All connections between email clients and the server must use TLS (encryption):
     - If you finished the “CA” (Certificate Authority) task, use the certificate you made for the mail server.
     - If not, create a self-signed certificate.
   - Make sure clients that trust “ITNSA Root CA” can verify the certificate.
3. LDAP Integration (User Login)
   - Configure the folder Maildir for user budi and boaz
   - Make sure the LDAP user named budi (created in the LDAP task) can:
     - Log in using his username(uid)
     - Access his email inbox
   - The email address should be taken from his mail field in LDAP.
   - Test email budi can send email to himself using mailutils

web-01.itnsa.id & web-02.itnsa.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 (10.10.20.100/24) that will automatically move to the backup server if the main server goes down.
   - web-01: acts as the MASTER with priority 101
   - 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: 10.10.20.21:8080
     - web-02: 10.10.20.22:8080
   - 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 on port 8080 with index.html “Hello from ${hostname}

Part 3 Firewall

The firewall server fw.itnsa.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.itnsa.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	10.10.20.100
443	TCP	10.10.20.100
53	TCP/UDP	10.10.10.10

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. Allowing all traffic incoming from interface MGMT
7. Block Everything Else
   - Any other traffic that’s not mentioned above should be blocked (default deny).

Wireguard VPN

Set up WireGuard as a VPN server so that an external workstation (client) can connect securely to the internal network.

1. Secure VPN Connection
   - Use WireGuard to create a secure tunnel from the client to the internal network.
   - All internet traffic from the client should be routed through the VPN tunnel.
2. Pre-Shared Key (PSK)
   - For extra security, add a pre-shared key to the tunnel (used along with public/private keys).
3. DNS Configuration
   - The client should use the internal DNS server (not public DNS) to resolve hostnames while connected.
4. IP Addressing
   - Use the IP range for the tunnel based on the General Configuration Table (ask or check your given network setup).
5. Save & Enable Configuration
   - Save the WireGuard config as:
     /etc/wireguard/wg0.conf

- Start it using:

  ```
  sudo wg-quick up wg0
  ```

- Enable it to run at boot (system service):

  ```
  sudo systemctl enable wg-quick@wg0
  ```

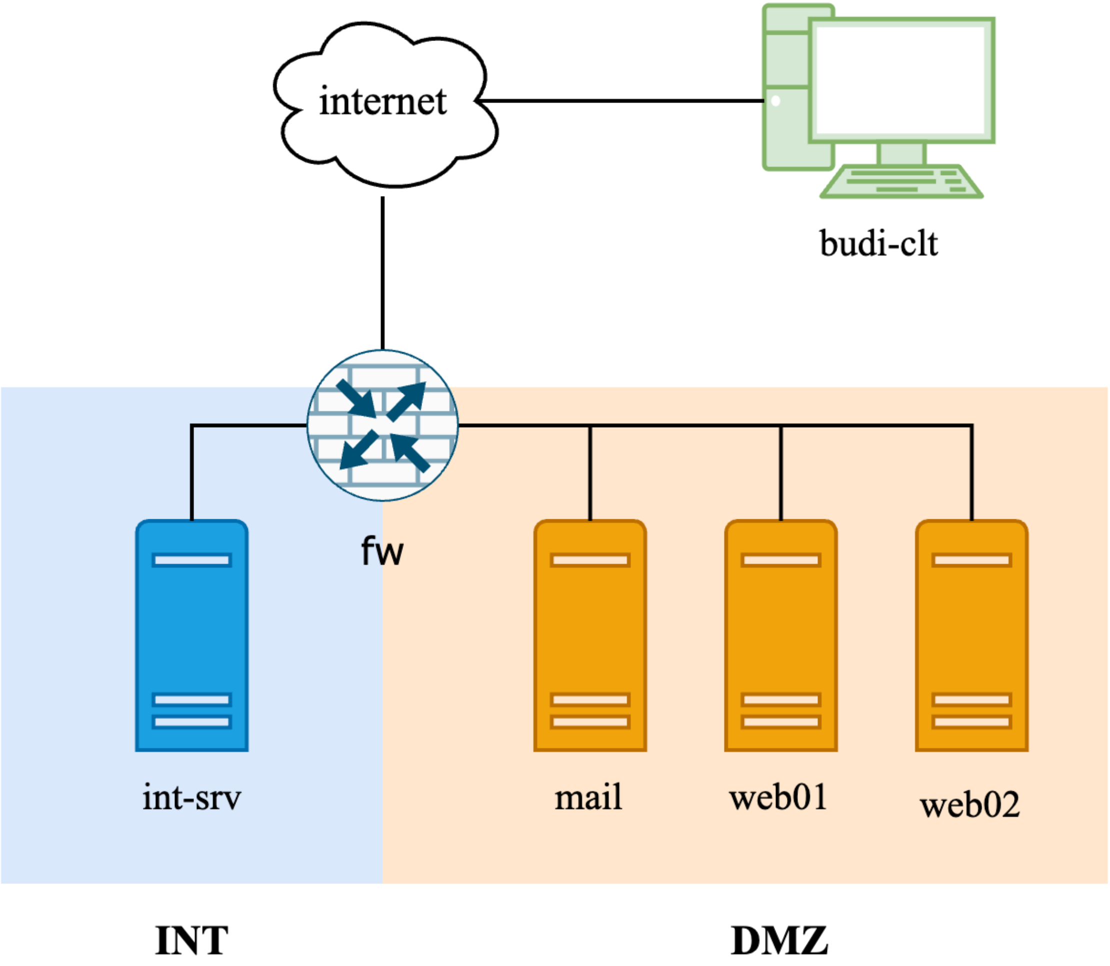
Part 4 Client

The client machine budi.itnsa.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 new local user budi (Budi Sudarsono), with the password “Skills39!”
   - Make user budi can sudoer without a password
2. Configure VPN WireGuard to fw.itnsa.id
   - Save the WireGuard config as:
     /etc/wireguard/wg0.conf
   - Start it using:
     sudo wg-quick up wg0
   - Enable it to run at boot (system service):
     sudo systemctl enable wg-quick@wg0
3. Can access https://www.itnsa.id via internet, and https://www.int.itnsa.id via vpn without getting errors certificate
4. Set up e-mail budi.sudarsono@itnsa.id in Thunderbird, and can send to himself

Topology


internet
budi-clt
fw
int-srv
mail
web01
web02
INT
DMZ