LOMBA KOMPETENSI SISWA

SEKOLAH MENENGAH KEJURUAN

TINGKAT NASIONAL XXVIII 2020

TEST PROJECT

IT NETWORK SYSTEMS ADMINISTRATION

LKS2020_LINUX_Actual

Contents

Part I – Basic Configuration

All of our servers and clients are using **debian 10.X**. All of our clients uses the default GNOME Desktop Environment. The following tools have been installed on each server and clients : **curl, ssh, smbclient, ftp, dnsutils,** and **sudo**.

The following requirements must be applied to all servers.

- Set and verify IP Address and Hostname for all devices according to the topology
- Make sure root login is not allowed.
- Make a user ‘kertarajasa’ with **sudo** privilege with password, as specified in the appendix.
- Please configure the domain-name and DNS resolver accordingly.

Part II – Infrastructure Management

Nusantara, inc. requires you to setup the following services with specified requirements.

Company web server at private.nusantara.id

- Use **nginx**, and please make sure it can serve php files.
- Serve **internal.nusantara.id** that requires LDAP authentication.
  - Display internal.php file by default with content listed in the appendix.
- Serve **public.nusantara.id** that is accessible without authentication.
  - Display index.php file by default with content listed in the appendix.
- Sync all the files to the company backup server.

Company file server at file.nusantara.id

- Using NFS version 4, please share the ‘/udd/home/’ directory for internal network.
- Permit root and/or owner of respective directories to read and write inside the directory.
- Create samba share /share/smb/ that requires LDAP authentication.
  - Make sure only the user ‘fatmawati’ that able to delete any file. Other users only allowed to upload and download files.

Company authentication server at file.nusantara.id

- Serve **LDAP** authentication backend.
- Create all users with all attributes listed in the appendix, along with their respective home directories.
- Make sure our internal services and/or clients are able to authenticate using this server.

Company mail server at private.nusantara.id

- Serve smtps at mail.nusantara.cloud port 465 with postfix.
- Serve imaps at mail.nusantara.cloud port 993 with dovecot.
- Make sure its accessible either via internal or external network.
- Use our Authentication Server to authenticate users, make sure their email address are usable like specified in the appendix.
- Encrypt these connections with self-signed SSL Certificate.

Company DNS at file.nusantara.id

- Create A records for all of Nusantara's internal servers.
- Create A records necessary for our websites and web-interface of our monitoring service.
- Create A records and MX records necessary for our email.

Company monitoring service at private.nusantara.id

- Please use **icinga2** and enable the web-interface at **monitor.nusantara.id**
- Monitor website accessibility of both **internal.nusantara.id** and **public.nusantara.id**
- Monitor our LDAP service availability.
- Monitor our site-to-site VPN tunnel connectivity.
- Configure email notification to **soedirman@nusantara.id** when any of these service are DOWN **as soon as possible**.

Part III – Security and Maintenance

The following are setup outside of Nusantara internal servers.

ITNSA backup server at se02.itnsa.id

- We recommend you to use **ssh** and **scp** for this task. However, you can also use other tools; as far as it works, we wouldn't complain.

- Configure our (Nusantara's) web server to upload their '/var/www/' content into this server at '/backup/www/'.
  - Do not change the directory structure
  - Using tools of your choice, make sure to sync **as soon as possible** (we tolerate max. ten seconds delay)
- Backup our LDAP database into '/backup/ldap/' every odd-hour using **cron** as **root**.

Company Firewall at fw.nusantara.id

The company requests you to use **iptables**

- Configure so that it will DROP all traffic by default
- Configure so that every internal service that requires access to outside are granted
- Configure nat for our **client.nusantara.id** internet access

Majapahit Firewall at fw.majapahit.net

The company requests you to use **iptables** even at this site.

- Configure so that it will DROP all traffic by default
- Configure so that every internal service that requires access to outside are granted
- Configure nat for our **Gajahmada-PC** internet access

Part IV Remote Connectivity

VPN Tunneling

- Configure **openvpn** site-to-site tunneling to connect Majapahit to our company.
- Use UDP port 1945 for connection.
- Use certificate authentication, create self-signed certificate as you wish.
- Make sure **client.nusantara.id** able to access all resource on Majapahit Zone
- Block traffic **from** Gajahmada-PC to Nusantara Zone via tunnelling
- Make sure Gajahmada-PC still able to access internet

Remote Access VPN

Configure remote access on **openvpn** for **Jane-laptop.** Use TCP port 1708 for this connection. Make sure the VPN Connection in **Jane-laptop** is available in the network manager with name **Krakatau**. Use LDAP for authentication. Make sure **Jane-laptop** able to access all resource on Nusantara Zone and Majapahit Zone after connection established.

Part V Company Services

Webmail Service on sa01.majapahit.net

- Use **roundcube** web-mail, and any web server of your choice.
- Use SSL self-signed certificate to serve HTTPS
- Make sure this webmail is accessible at the internet address **https://webmail.majapahit.net**
    - you need to configure Majapahit firewall to make this work.
- At login prompt, user are able to choose 2 MAIL server, Nusantara and ITNSA.
- If Nusantara is chosen, user will connect to Nusantara's mail server. You may need configure the Nusantara firewall in order to make this work.
- If ITNSA is chosen, user will connect to ITNSA's mail server on the internet.
- make sure user can send/receive email to/from ITNSA and Nusantara mail servers.

FTP Service on sa01.majapahit.net

- Use **proftpd**
- Publish this ftp so that it is accessible via the internet address of **ftp.majapahit.net**
- Allow both implicit **ftps** and plain **ftp**
- Disallow anonymous login, use local user database to authenticate users. Please refer to appendix.
- Permit download and upload of new file for users, make sure they cannot delete any file(s) on the server.

Public Mail service on se01.itnsa.id

- Use **dovecot** and **postfix**
- Serve smtps at mail.itnsa.id port 465 with postfix. Use STARTTLS Auth.
- Serve imaps at mail.itnsa.id port 993 with dovecot. Use STARTTLS Auth.
- Use local user database to authenticate users, please refer to appendix. Make sure user's email address are the same as the one listed in appendix.
- Encrypt these connections with self-signed SSL Certificate.
- Configure an autoreply user **no-reply@itnsa.id**, whenever this user receives an email, an automatic reply must be sent immediately.
  - The message subject is *Automatic Reply from itnsa.id*
  - The message body is :
    Your inquiry has not been read by any of our personnel. Kindly visit http://itnsa.id for more information on how to contact us.

Public DNS on ITNSA Zone.

- Use **bind9**
- Serve records for **itnsa.id** domain. Create subdomains needed for mail service to work, both A record and MX record.
- Serve records for **majapahit.net** domain. Create subdomains needed for webmail service and ftp to work, both A record and MX record.
- Create master-slave relationship with following detail:
  - Master: **se01.itnsa.id**

  - Slave: **se02.itnsa.id**
  - Encrypt slave-master zone updates using DNSSec key – Transaction Signature.
  - Whenever record at the master is updated/changed, the record at the slave must also be updated/changed.

DHCP Service

- Majapahit DHCP Server (**sa01.majapahit.net**)
- Create pool for Majapahit clients with following requirements:
- Range : 10.20.19.10-10.20.19.100
- DNS : 172.45.80.3
- Set gateway accordingly

Nusantara DHCP Server (fw.nusantara.id)

- Create static IP lease for Jane-laptop (178.45.80.4/28). Configure DNS and Gateway accordingly.
  - Enable Dynamic DNS to the DNS service at ITNSA zone. Secure the transaction using DNSSec and make sure the record is automatically replicated to the slave DNS.
- Create pool for Nusantara clients. There are no specific rule, just make sure the client can access our services without any problems.

Nusantara Remote Login

- Allow the PC **client.nusantara.id** to login with LDAP credentials stored in the company's Authentication Server
- Disable local user to login on this PC, so the user will be forced to use their company account stored in the Authentication Server. root should still be able to login just fine on the terminal. Note: on the GUI, root login is disabled by default, you shouldn't mess with this.
- Mount the NFS share at our file server automatically to '/udd/home' upon boot. This will be the LDAP users' homedir when they login remotely, so please configure the permissions accordingly and make sure it works like usual homedir.

Appendix

LDAP_Users

username	password	homedirectory	emailaddress
fatmawati	Skill39	/udd/home/fatmawati	fatmawati@nusantara.id
malakatan	Skill39	/udd/home/malakatan	malakatan@nusantara.id
soedirman	Skill39	/udd/home/soedirman	soedirman@nusantara.id
mohhatta	Skill39	/udd/home/mohhatta	mohhatta@nusantara.id

Local_Users

username	password	homedirectory	emailaddress
kertarajasa	Skill39	/home/kertarajasa	kertarajasa@itnsa.id

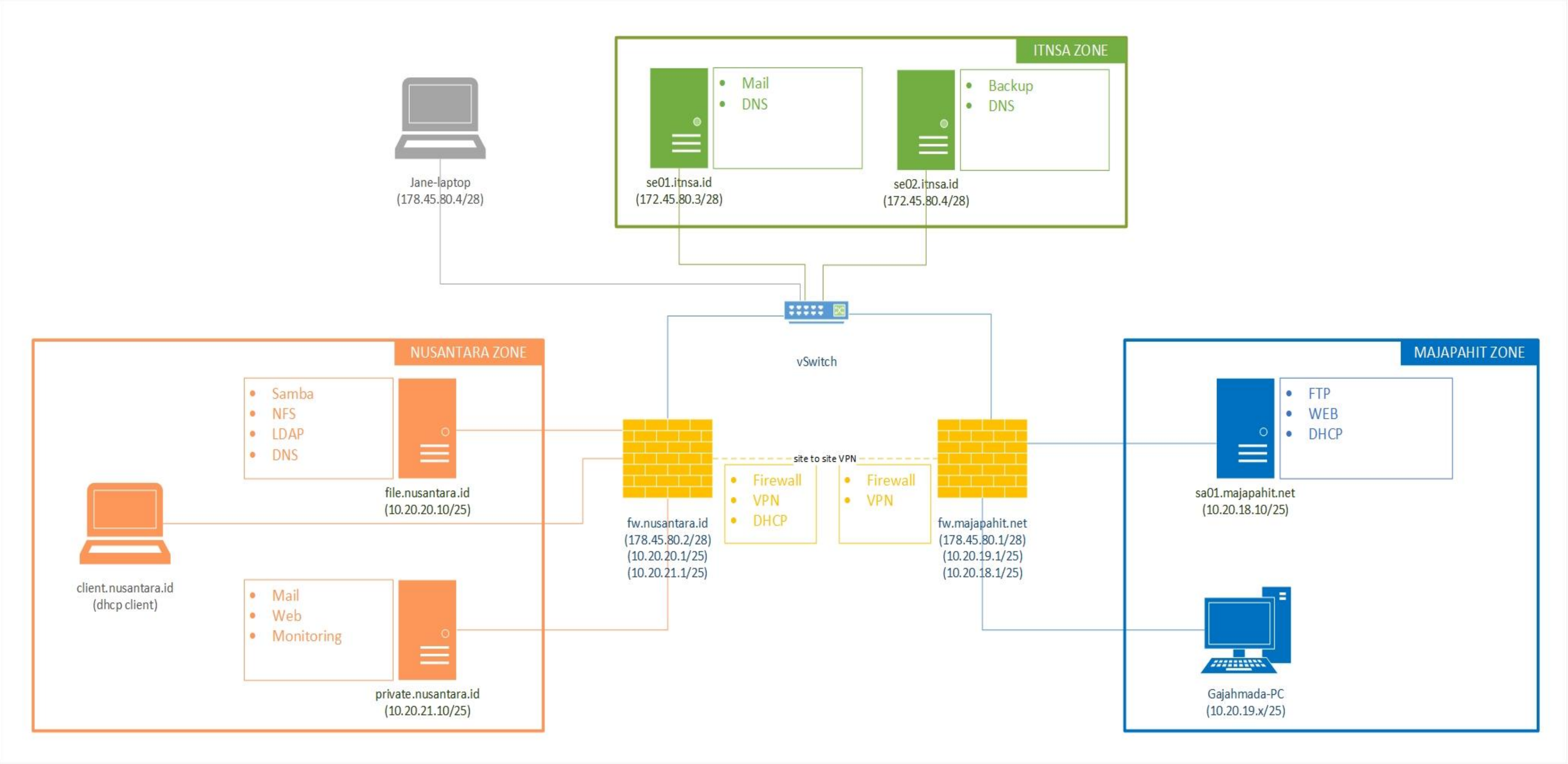
internal.php

```
<?php
 echo “Internal access only. Hosted on ” . gethostname();
?>
```

index.php

```
<?php
 echo “Welcome to Nusantara public access.”;
?>
```

Topolog


ITNSA ZONE
Mail
DNS
se01.itnsa.id
(172.45.80.3/28)
Backup
DNS
se02.itnsa.id
(172.45.80.4/28)
Jane-laptop
(178.45.80.4/28)
vSwitch
NUSANTARA ZONE
Samba
NFS
LDAP
DNS
file.nusantara.id
(10.20.20.10/25)
client.nusantara.id
(dhcp client)
Mail
Web
Monitoring
private.nusantara.id
(10.20.21.10/25)
site to site VPN
Firewall
VPN
DHCP
fw.nusantara.id
(178.45.80.2/28)
(10.20.20.1/25)
(10.20.21.1/25)
Firewall
VPN
fw.majapahit.net
(178.45.80.1/28)
(10.20.19.1/25)
(10.20.18.1/25)
MAJAPAHIT ZONE
FTP
WEB
DHCP
sa01.majapahit.net
(10.20.18.10/25)
Gajahmada-PC
(10.20.19.x/25)