TEST PROJECT
MODULE A

IT NETWORK SYSTEMS ADMINISTRATION

KELOMPOK INFORMATION AND COMMUNICATION TECHNOLOGY

LOMBA KOMPETENSI SISWA
SEKOLAH MENENGAH KEJURUAN
TINGKAT NASIONAL KE XXX
TAHUN 2022

Deskripsi

A branch of a big company has hired you to configure their newly built infrastructure.There will be three sites, DMZ, Internal, and Edge. They will use both Windows and Linux for their services. Attached the logical topology of the new branch infrastructure.

Credentials

Debian
username : root
password : Skills39

Windows 10
username : competitor
password : Skills39

Windows Server
username : Administrator
password : Skills39

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.

Supporting Services

DHCP and Network Booting

- NF will serve as both DHCP Server and TFTP Server. You can freely use any tools to provide the service.
    - Configure TFTP server at NF to provide boot images for debian OS.
    - Configure NF 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 NF.
- 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 Load Balancing

- Configure NF 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 log in single file: /var/log/firewall.log
- Configure NF using haproxy to load balance incoming HTTPS traffic using algorithm that divides the load evenly to MON1 and MON2 servers.
    - Use the default config file: /etc/haproxy/haproxy.cfg.
    - Get the required certificate to enable HTTPS.
    - Make sure icinga monitoring web UI is accessible via this service.
- Create simple firewall rule in EDGE1 and EDGE2 to block these traffic:
    - From NF to SERVICE1 via HTTP and HTTPS port.
    - From NF to SERVICE2 via HTTP and HTTPS port.

Routing and NAT

- Enable routing in NF, EDGE1 and EDGE2.
- Enable port NAT in NF to allow EDGE1, EDGE2, and Internal Servers to reach public network.
- Route traffic from Internal to NF, 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: 172.16.34.124/25
    - Do not route traffic from the public network.
- Route traffic from DMZ to NF, 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: 10.99.99.252/24
    - Do not route traffic from the public network.

Monitoring

- Configure centralized monitoring using icinga2 hosted in MON1 and MON2.
    - Enable web interface, make it accessible using port 80 from either hosts.
        - Make sure it's accessible via mon.itnsa.id
    - Enable High Availability feature on icinga2 on both servers so that if one server fails, monitoring will still be able to function normally.
- Configure monitoring for services and servers
    - Add mail and webmail services to be monitored in icinga2
    - Add SSH services in all linux servers in both Internal and DMZ to be monitored in icinga2
    - Configure mail notification to notification@itnsa.id whenever any of the monitored services are down for more than 1 minute.
        - If you are unable to configure the mail group, send it to ops@itnsa.id instead.
    - Set email text as you see fit, with required information like alert type and server IP.
- Configure monitoring for failed SSH Logins in all linux servers
    - Configure mail notification to ops@itnsa.id whenever someone fails to login using SSH.
    - Set email text as you see fit, with required information like alert type and server IP.
- Configure monitoring for all windows servers.
    - Configure mail notification to ops@itnsa.id whenever any of the servers is powered off.
    - Set email text as you see fit, with required information like alert type and server IP.

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

Certificate Authority

- Configure MAIL as Root CA.
    - Use Common Name: LKSN2022-Root
    - Approve Intermediate CA Requests for MON1 and MON2.
    - Save those two Intermediate CA certificate files without the key in directory /backup in MAIL server.
- Configure MON1 as Intermediate CA Issuer.
    - Use Common Name: LKSN2022-Intermediate-1
- Configure MON2 as Intermediate CA Issuer.
    - Use Common Name: LKSN2022-Intermediate-2
- In any of the Intermediate CA, issue the certificates required for other services.
    - For record, place all generated certificates in /backup/certs in MAIL server.

Main Services

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 MON1 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 NF to test the VPN Client connection, but please don’t keep the connection running.
    - Distribute client configuration file to connect to NF in /etc/openvpn/client.ovpn

OS Configuration

- We’ve wrongly configured the / partition at STORAGE, please increase the partition to use 100% of the available disk.
- 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

Main Website

- Configure SERVICE1 and SERVICE2 to hosts all departement’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 Corporate 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 SERVICE1 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
        - Monitoring
    - Set NS record for the domain to SERVICE1 and SERVICE2.
- Copy all records in SERVICE1 to SERVICE2, allowing SERVICE2 to serve as failover DNS.

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 STORAGE1 and STORAGE2 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	IP Address	Preinstalled
EDGE1	Windows Server 2019 desktop	10.99.99.253/24	yes
		172.16.34.125/25	
		10.199.99.252/28	
EDGE2	Windows Server 2019 desktop	10.99.99.254/24	yes
		172.16.34.126/25	
		10.199.99.253/28	
SERVICE1	Windows Server 2019 desktop	172.16.34.11/25	yes
SERVICE2	Windows Server 2019 desktop	172.16.34.12/25	yes
NF	Debian 11 Server	10.199.99.254/28	yes
		202.29.195.25/30	
OPS	Windows 10	172.16.34.10/25	yes
		202.29.195.26/30	
MON1	Debian 11 Server	10.99.99.21/24	yes
MON2	Debian 11 Server	10.99.99.22/24	yes
MAIL	Debian 11 Server	10.99.99.25/24	yes
STORAGE	Debian 11 Server	172.16.34.15/25	yes
OFFICE	None	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

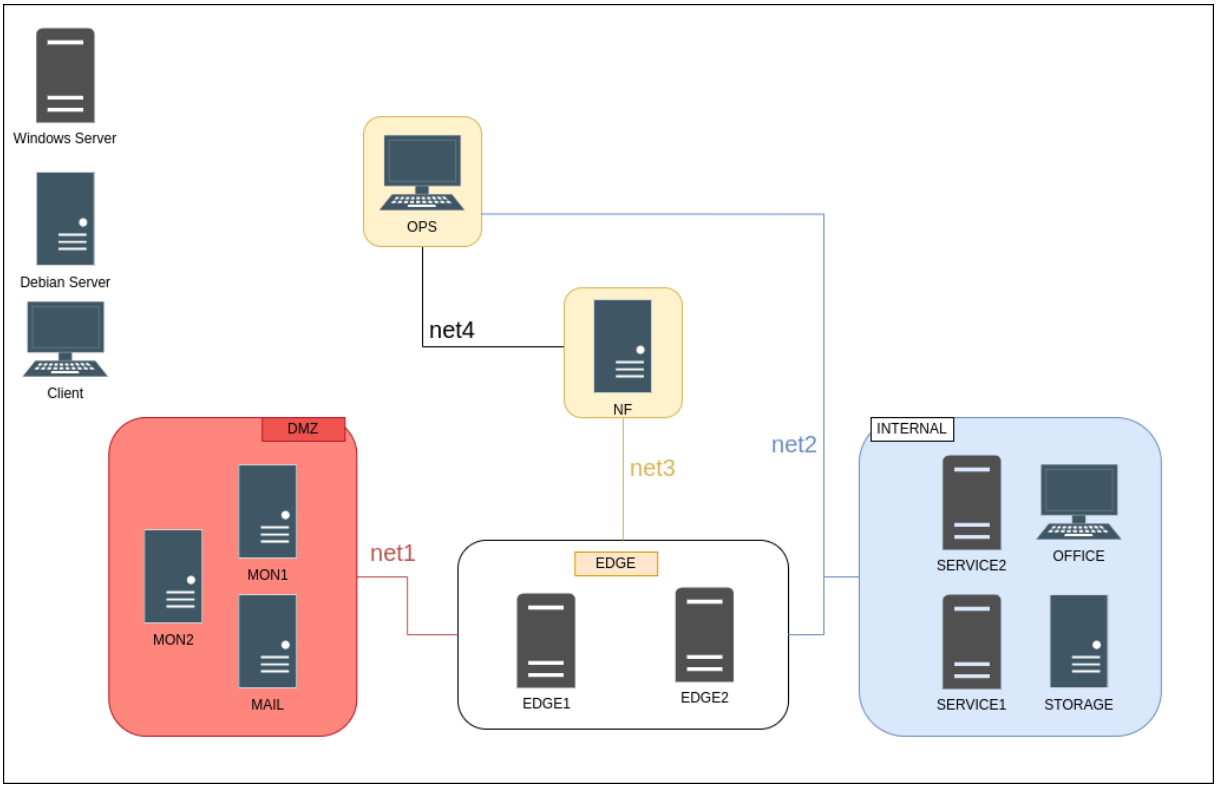
```
<h1> dev.itnsa.id </h1>
This website is managed by dev@itnsa.id
```

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


Windows Server
Debian Server
Client
OPS
net4
NF
net3
net2
DMZ
MON1
MON2
MAIL
net1
EDGE
EDGE1
EDGE2
INTERNAL
SERVICE2
OFFICE
SERVICE1
STORAGE