Module Linux
Seleksi Calon Competitor
World Skills Competition 2021 Shanghai

BASIC CONFIGURATION ON ALL SERVERS

Login Banner

- Must be shown before the login prompt. Must appear for local and network logins.
  - Welcome to <hostname> - PRA-TC ITNSA 2020
- Create a script /root/banner.sh to add the hostname dynamically. The script must be executed at every reboot.

OFFICE AND HOME NETWORK

fw1.itnsa.id

- Site to Site VPN
  - Configure site-to-site IKEv2 VPN to fw2.itnsa.id using StrongSWAN all traffic between the office.
  - Network and the public cloud network should be routed through the tunnel.
- OpenVPN Remote Access
  - Configure client VPN for janes-pc. When connected the user should have the same access to all resources as clients in the office and home network. This includes the private cloud network and public cloud network.
- IPTABLES
  - Default policy for any traffic through the firewall should be DROP.
  - Bypass or whitelist any traffic from office network.
  - Implement NAT overloading for traffic from office and home network to internet, use custom chain named INTERNET.
  - HTTPS traffic from remote access VPN network to private cloud network should not be routed via site-to-site VPN.
  - Add all necessary rules so the services working as intended
- DHCP

- Configure DHCP for office and home network. Add A and PTR records automatically to file.itnsa.id Make sure that file.itnsa.id are always assigned the same address.

file.itnsa.id

- DNS

o Configure a forward zone called “itnsa.id”.
o Create A Record for all host defined in the ITNSAID Zone (Except intclient).

  - Add a CNAME record for “public” that points to the proxy server in this zone.
  - Add a CNAME record for “landing” that points to the web server which is handle the landing page for RPZ.
  - Add a A record for “mail” that points to the mail server IP address in this zone.
  - Create an appropriate MX Record.
  - Add a CNAME record for “vpn” that points to the vpn server in this zone.
  - Add a CNAME record for “files” that points to the file server in this zone.
  - Add a CNAME record for “monitor” that points to the monitoring server in this zone.

o Create Reverse Zone defined for the Office and Home Network and the Private Cloud Network.
o Configure the DNS RPZ (Response Policy Zone) :

  - Block the malicious domain: malicious.com.
  - When visiting the malicious domain via web browser, the user should have redirected to the landing.itnsa.id webpage. And all queries to malicious domain should redirected to landing.itnsa.id.

o All other queries (not in this domain) should forwarded to isp1.worldskills.org.

- LDAP

o Configure LDAP service for itnsa.id and worldskills.org domain.
o Add all user entries with attribute based on the table in the appendix. The LDAP user will be used for service and local machine authentication.

- RAID

Add three extra hard drives each 1GB in size. Configure a RAID 5 array /dev/md0.

- LVM

Add /dev/md0 as physical volume and make logical volume /dev/file/data. Create necessary volume

group and mount the logical volume on /files.

- DISTRIBUTED FILE SHARE (DFS)

- o Configure Samba for DFS
- o Enable DFS.
- o DFS should be accessible through “\\files.itnsa.id\dfs”
  - o Local DFS root : /files/dfs.
- o Distribute share “public” through DFS
  - o Remote path : \\files.itnsa.id\public.
- o Distribute share “internal” through DFS
  - o Remote path : \\files.itnsa.id\internal.
- o Configure share “public” :
  - o Local path : /files/public
  - o Give read only access to everyone
  - o Make sure the share not visible on the network
- o Configure share “internal” :
  - o Local path : /files/internal
  - o Give write access to everyone
  - o Allow only Home and Office network and Private Cloud Network to access this share
  - o Make sure the share not visible on the network

- Monitoring

- o To monitor the network setup Icinga2. The web-interface must be accessible on port 8080 and listen for any hostname/ip. Use the username icingaadmin with the password Passw0rd$. Add the following checks:
  - o Monitor fw1.itnsa.id using ICMP.
  - o Monitor the status of the website intranet.itnsa.id.

janedoe.itnsa.id

Add the PRA-TC ITNSA 2020 CA as trusted root certificate. And retrieve needed certificate for this client to access the services. Make sure no certificate warning shown when accessing the services.

- LDAP Client

o Make sure the LDAP user in itnsa.id domain can login locally.
o Add offline capabilities. When LDAP Server can't be accessed, it should be able to login with the cached LDAP credentials.
o After LDAP is offline, it should still be possible for users to access the host within one minute

- E-Mail Client

o Use Icedove as the e-mail client and configure using the user "skill39"
o Configure using anne@itnsa.id mail account.
o Send a mail to mark@worldskills.org. Don't delete these mail.
o Configure the mailbox using IMAP with TLS.

- Web Client

o Make sure the client can open the public.itnsa.id in the web browser without certificate warning shown (HTTPS). Show the appropriate content.
o When opening the malicious.com in the web browser, it should be redirected to landing.itnsa.id webpage.

Private Cloud Network

fw2.itnsa.id

- Site to Site

Configure site-to-site IKEv2 VPN to fw1.itnsa.id - office and home network.

- IPTABLES

o All traffic through the firewall should be blocked by default.
o Traffic to and from private.itnsa.id should be hidden behind the external IP-address.
o Add all necessary rules for the services and tunnels to work as intended.

- Reverse Proxy (Nginx)

  - Install and configure Nginx as the HTTPS Proxy for public.itnsa.id.
  - Use the certificate issued by isp1.worldskills.org.
  - All HTTP request should be redirected to the HTTPS automatically.

private.itnsa.id

- Email

  - Configure the server to send and receive emails for all the office users under the domain itnsa.id.
  - The users should be able to access their mailbox via IMAP. All communication between this server
  - and the clients should be secured with TLS (STARTTLS).
  - It should be possible to send e-mails to users in the worldskills.org domain.

- WEB

Install an Apache2 webserver and serve the site intranet.itnsa.id. Use /www/intranet as the document root. The office users should be authenticated using the LDAP-server on file.itnsa.id.

  - This is server [hostname]. Welcome, [username]

- Host a basic HTTP Web for landing.itnsa.id.

  - The webpage should display the message below : “WARNING : You are tried to visit malicious domain web. Access has been denied.”
  - Add the public.itnsa.id web and enable HTTPS only site on this web :
    - Root directory is /files/web/public
    - Use certificate issued by isp1.worldskills.org.
    - When visiting public.itnsa.id, directory listing of /files/web/public should be displayed.
    - As a basic security measure, make sure no sensitive information displayed in the HTTP header and footer.

- Backup

  - Backup /important-data to srvpv02.fast-provider.net using rsync. This should be done every 10 minutes (use the crontab of root). Create a script /usr/local/bin/backup.sh that can be used to run the backup manually.

- SSH

To make it possible to manage the website intranet.itnsa.id add a user called webmaster with the password Passw0rd$ and give it SSH and SFTP access. The users home directory should be the same as the document-root of the website. The user should not be allowed to leave the home directory. The user should only be allowed to use the command ping.

Public Cloud Network

isp1

- DNS

Configure DNS zones for worldskills.org . Add all necessary entries. Request for itnsa.id should be forwarded to file.itnsa.id

- CA (Openssl)

o Configure CA using OpenSSL.
o Use /etc/ca as the CA root directory.
o Private key should have minimal permission.
o CA attributes should be set as follows :
o Country is set to ID.
o Organization is set to WorldSkills International.
o Common Name is set to “PRA-TC ITNSA 2020 CA”.
o Create a root CA certificate.
o All certificates required in the test project should be published by this CA.

- MAIL SERVER

o Install Postfix and Dovecot.
o Configure SMTPS and IMAPS server for "worldskills.org” domain using certificates issued by this server.
o Configure mail directory in /home/[user]/Maildir.
o Authentication has to be done through LDAP (worldskills.org domain).
o Make sure that the corresponding local user do not exist
o The corresponding LDAP user for mail authentication should restricted to the local login.
o Enable SMTP submission (TLS TCP/587).
o Disable port TCP/25.
o Enable secure IMAP (TLS TCP/143).
o The mail communication to the itnsa.id domain should be possible.

isp2

- DNS

Setup the DNS-server to be a secondary server for the zone worldskills.org . When adding entries to the primary server, they should automatically synchronize.

- rsync backup

o Install and configure rsync backup service. The server private.itnsa.id should be configured to make scheduled backups (use the crontab of root) to the /backup/private-itnsa-id folder.
o Perserve the directory structure.
o Make sure that only the file owner can read the files in /backup.
o As a basic security measure, make sure that only clients from the private cloud are allowed to synchronize. Unauthorized access should be logged to /var/log/rsync/rsync-access.log.

johndoe

- Openvpn Client

o Install and configure the OpenVPN Client. Use the OpenVPN Client that can be used
o for GNOME Network Manager.
o Make sure the VPN Connection can be established to fw1.itnsa.id. After that, this client should be able to access the service in the next task.

- Email Client

o Use Icedove as the e-mail client and configure using the user “skill39”
o Configure using mark@worldskills.org mail account.
o Send a mail to anne@itnsa.id. Don’t delete these mail.
o Configure the mailbox using IMAP with TLS.

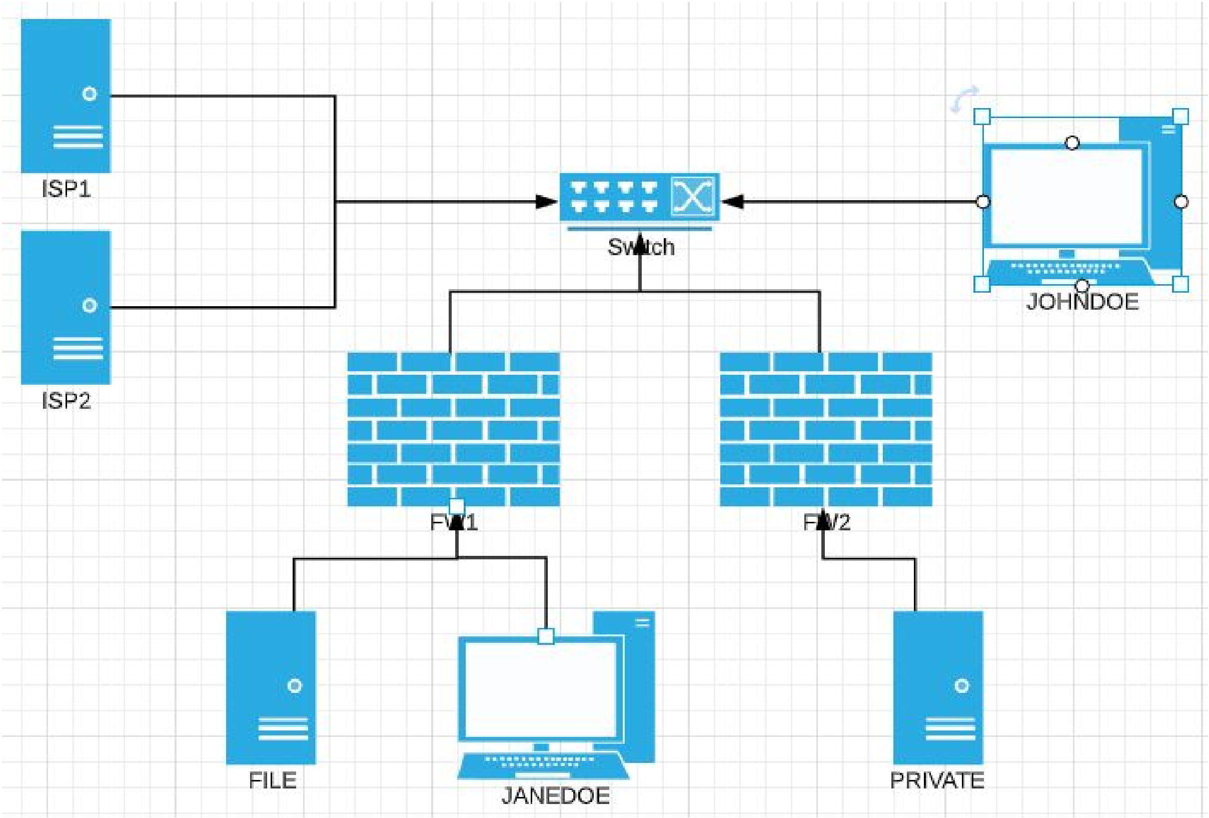
Appendix I : LDAP Users

username	password	domain	homedirectory	emailaddress
anne	Skill39	itnsa.id	/home/anne	anne@itnsa.id
mark	Skill39	worldskills.org	/home/mark	mark@worldskills.org

Appendix II : IP Addressing Table

fqdn	IP Address	zone
isp1.worldskills.org	212.11.22.3/29	WORLDSKILLS
isp2.worldskills.org	212.11.22.4/29	WORLDSKILLS
fw1.itnsa.id	170.17.51.1/24 212.11.22.1/29	EDGE
janedoe.itnsa.id	DHCP	ITNSAID
file.itnsa.id	DHCP 170.17.51.2/24	ITNSAID
private.itnsa.id	170.16.11.2/25	ITNSAID
fw2.itnsa.id	170.16.11.1/25 212.11.22.2/29	EDGE
johndoe	212.11.22.5/29	ITNSAID

Appendix III : Topology


ISP1
ISP2
Switch
JOHNDOE
FW1
FW2
FILE
JANEDOE
PRIVATE