Seleknas ASC XIII - Linux

General Configuration

- Set all hostname and IP according to the appendix.
- Use password **Skills39** unless specified.
- Install the following software on all hosts:
    - curl
    - dnsutils
    - ldap-utils
    - lftp
    - lynx
    - nfs-common
    - traceroute
    - tcptraceroute
    - smbclient

Office Network

The network that will be used for office works and tasks. You need to configure this network so it is easy for the office workers to collaborate. For security purpose you are also tasked to configure the firewall and the connection to upstream ISP.

fw.skill39.net

This is the firewall for office and private cloud network.

VPN

- Use **OpenVPN** as VPN software.
- Configure site-to-site VPN to **fw.worldskills.org**:
- Use **layer 3 device** and **connectionless** protocol with port **1195**.

- Place traffic from **office network** to **public cloud network** into the VPN tunnel.

- Setup remote access VPN:
    - Use OpenVPN default port.
    - LDAP as authentication backend.
    - IP range **10.99.99.100-10.99.99.120** and subnet mask **255.255.255.0**.

    - VPN Clients have access like office network.

DHCP Server

- Configure DHCP service for office network, push dns and ntp server to clients.

- Any lease should update the A and PTR records on **file.skill39.net**.
- **client1.skill39.net** is always assigned IP address **192.168.1.10**.

Firewall

- Use **iptables** as firewall backend.
- 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 private cloud network to internet, use custom chain named INTERNET.
- HTTPS traffic from remote access VPN network to public cloud network should not be routed via site-to-site VPN.
- Add all necessary rules so the services working as intended.

file.skill39.net

This is the authentication and file server for the office network.

LDAP

- Use **openLDAP** as LDAP server software.
- Configure the LDAP objects according to the appendix.

RAID

- Add three additional virtual disks.
- Create a **RAID 5** block device using the additional disks.

LVM

- Add **/dev/md0** as physical volume.
- Create logical volume **/dev/file/data** from the physical volume.
- Mount the logical volume on **/data**

SAMBA

- Create a share with the following specifications:
  - Name: **public-files**
  - Path: **/data/public-files**
  - Allowed host: **public.worldskills.org**
  - Permissions: read-only

NFS

- Create the documents share with specifications:
  - Path: /**data/documents**
  - Permissions: Read-write
  - Export only for office network.
- Share a home directory for each office users in LDAP database. The home folders should only be accesible by the respective users.

DNS

- Use **bind9** as DNS server software.
- The server should be the authoritative server for domain **skill39.net**, and add necessary records.
- Configure reverse lookup zone for office and private cloud networks.
- Any other lookup should be forwarded to to **srvpv01.fast-provider.net**

client1.skill39.net

This machine will be the primary client used for testing purpose on office network.

Client configuration

- Only **root and LDAP users** should be able to login locally (CLI and GUI).
- Mount the nfs share **documents** to **/mnt/documents**.
- Each home folders of LDAP users should be accesible after login.
- Configure the **Thunderbird** mail client for user "adam" to send and receive mail for **adam@skill39.net**.
- Make sure root CA certificate from **srvpv02.fast-provider.net** is trusted by system or any other software (firefox, thunderbird).

Home network

This network will be used to simulate a remote worker connected via internet.

extclt

This machine will be use to test the remote access vpn and external access from internet.

Client configuration

- Create a script **/usr/local/bin/startup.sh** to create an empty file **/last-boot**.
- Create a systemd service named **loglastboot** that run the script at system startup.
- Create local user **jane**:
  - Configure mail client **Thunderbird** to send and receive mail.
  - Configure VPN connection to **fw.skill39.net**.
- Make sure root CA certificate from **srvpv02.fast-provider.net** is trusted by system or any other software (firefox, thunderbird).

Private cloud

The private cloud is used to provide public services to the office users. For security purposes it is isolated in its own network segment.

private.skill39.net

Certificate authority

- Certificate files should be located on **/certs**
- Make sure the Sub CA with specifications:
  - Country: ID
  - Organization: skill39.net
  - Common Name: skill39 Sub CA
  - Public Key: subca.crt
  - Private Key: subca.key
  - Signed by root CA on **srvpv02.fast-provider.net**
- Use this sub CA to publish certificates needed for another services.

Mail server

- Use postfix and dovecot as mail server software.
- Setup mail system for domain **skill39.net**.
- Use encrypted protocol (STARTTLS) using certificate signed by Sub CA.
- Sendimg mail to domain **worldskills.org** should be possible.

Database server

- Use mariadb as database server.
- Import **db.sql** to database **db_skill39**.

Web server

- Use **apache2** as server software.
- Configure site **intranet.skill39.net** with files located on **/srv/intranet**.
- Use file **intranet.html** as index file with content "Welcome to intranet site."
- Users should authenticate with LDAP user before accessing the site.

Backup

- Create script named **/usr/local/bin/backup.sh** to backup **/srv/intranet/** to **srvpv02.fast-provider.net** using rsync.
- Run the script every odd minutes by using system crontab.

Public cloud

This network is used to host the production services that will publicly accessible.

fw.worldskills.org

VPN

- Configure site-to-site VPN in order to complete the configuration on **fw.skill39.net**.

Firewall

- Use **iptables** as firewall backend.
- Default policy for any traffic through the firewall should be **DROP**.
- Traffic from **public.worldskills.org** to internet (and vice versa) should be hidden behind external IP address of the firewall.
- Add all necessary rules so the services working as intended.

public.worldskills.org

This server will provide services that is publicly accessible.

SAMBA

- Mount **/data/public-files** on **file.skill39.net** to local directory **/data/public-files**.

Web server

- Use **apache2** as web server software.
- Configure site **www.worldskills.org**:
    - Directory: **/home/webmaster**
    - index.html content: "Welcome to www.worldskills.org".

FTP server

- Use **vsftpd** as server software.
- Create local user **webmaster**, use root directory of web **www.worldskills.org** as home folder.
- Jail the user in their home directory.
- Uploaded files should be owned by user and group **www-data**.
- Enable **explicit TLS** using certificate signed by **skill39 Sub CA**.

Service Provider

The service provider network represents the internet in this scenario.

srvpv01.fast-provider.net

This server provide ISP related services.

DNS

- Use bind9 as DNS server software.
- Configure zone **worldskills.org** and **fast-provider.net**, add all necessary entries.
- Request for **skill39.net** should be forwarded to **file.skill39.net**.

Mail server

- Use **postfix** and **dovecot** as mail server software.
- Setup mail system for domain **worldskills.org**.
- Add local user **jane**.

- Use encrypted protocol (STARTTLS) using certificate signed by **skill39 Sub CA**.
- Sending mail to domain **skill39.net** should be possible.
- Configure echo@worldskills.org to auto-reply mail to sender for every incoming mail.

NTP

- Sync clock with NTP server on **srvpv02.fast-provider.net** using package **ntp**.

srvpv02.fast-provider.net

This server is used as remote backup.

Backup

- Install **rsync**.
- Backup from **private.skill39.net** should be located on **/backup/private-skill39-net** folder.
- Make sure that only the file owner can read the files in /backup.

Certificate authority

- Certificate files should be located on **/certs**
- Setup a root CA with specifications:
  - Country: ID
  - Organization: Fast Provider
  - Common Name: Fast Provider Root CA
  - Public Key: rootca.crt
  - Private Key: rootca.key
- Use this root CA to **only** sign certificate of sub CA on **private.skill39.net.**

NTP

- Use **ntpd** as ntp server.

- Configure local clock as the only time source.

Appendix

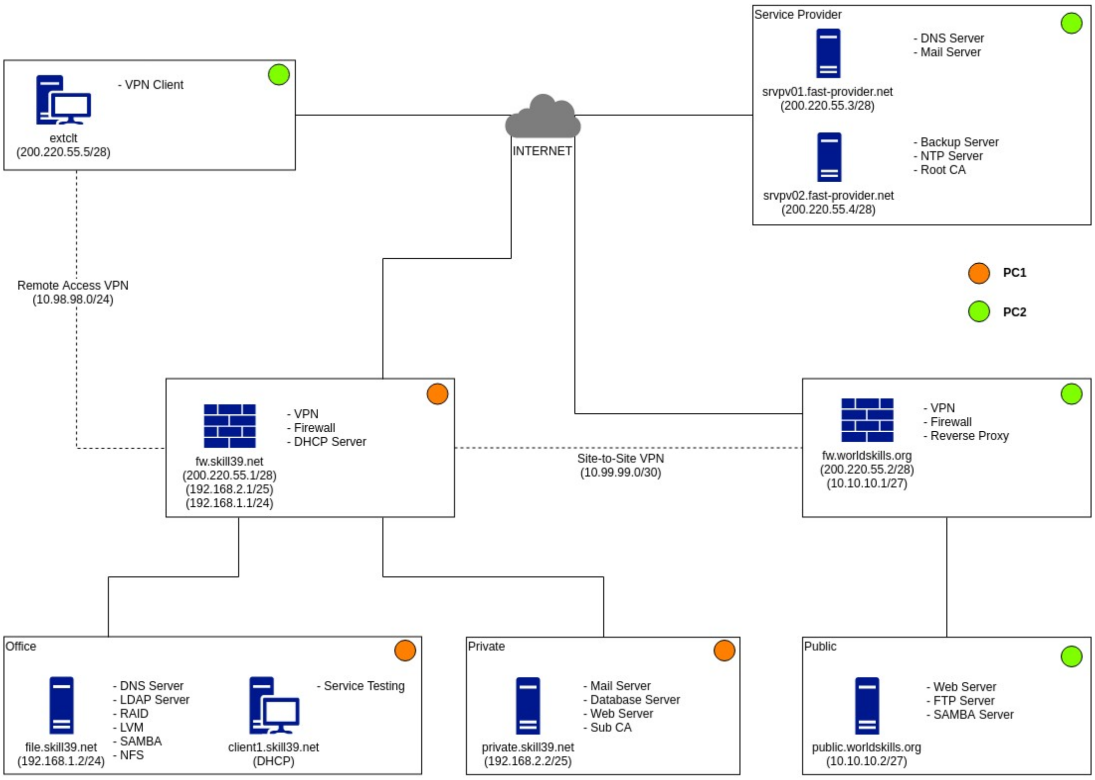
Office Users

Username	Email	Home Folder
adam	adam@skill39.net	/mnt/homes/adam
jane	jane@worldskills.net	/mnt/homes/jane

Hosts

Hostname	IP Address	Services
fw.skill39.net	200.220.55.1/28 192.168.1.1/24 192.168.2.1/25	DHCP, Firewall, VPN
file.skill39.net	192.168.1.2/24	DNS, LDAP, NFS, SAMBA
client1.skill39.net	192.168.1.10/24 (DHCP)	---
private.skill39.net	192.168.2.2/25	Mail, Sub CA, Web
fw.worldskills.org	200.220.55.2/28 10.10.10.1/27	Firewall, VPN
public.worldskills.org	10.10.10.2/27	FTP, Web
srvpv01.fast-provider.net	200.220.55.3/28	DNS, Mail
srvpv02.fast-provider.net	200.220.55.4/28	Backup, NTP, Root CA
extclt	200.220.55.5/28	---

Topology


Service Provider
- DNS Server
- Mail Server
srvpv01.fast-provider.net
(200.220.55.3/28)
- Backup Server
- NTP Server
- Root CA
srvpv02.fast-provider.net
(200.220.55.4/28)
- VPN Client
extclt
(200.220.55.5/28)
INTERNET
Remote Access VPN
(10.98.98.0/24)
PC1
PC2
- VPN
- Firewall
- DHCP Server
fw.skill39.net
(200.220.55.1/28)
(192.168.2.1/25)
(192.168.1.1/24)
Site-to-Site VPN
(10.99.99.0/30)
- VPN
- Firewall
- Reverse Proxy
fw.worldskills.org
(200.220.55.2/28)
(10.10.10.1/27)
Office
- DNS Server
- LDAP Server
- RAID
- LVM
- SAMBA
- NFS
file.skill39.net
(192.168.1.2/24)
- Service Testing
client1.skill39.net
(DHCP)
Private
- Mail Server
- Database Server
- Web Server
- Sub CA
private.skill39.net
(192.168.2.2/25)
Public
- Web Server
- FTP Server
- SAMBA Server
public.worldskills.org
(10.10.10.2/27)