worldskills

Test Project

Module A - Linux Environment

IT Network Systems Administration

Submitted by:
Ahmad Reza Mollapour, Independent Test Project Designer
Fabian Flückiger, Independent Test Project Validator

Contents

Introduction **3**
Description of project and tasks **4**
General Configuration 5
Part 1: Shenzhen Servers **8**
Work Task: SSL/TLS Certificate 8
Work Task: Server szx-gw-1 8
Work Task: Server szx-srv-1 9
Work Task: Server szx-srv-2 10
Work Task: Server szx-srv-3 11
Work Task Server sha-gw-1 13
Part 3: Clients **14**
Work Task szx-clt-1 14
Work Task sha-clt-1 14

© WorldSkills International

Introduction

Welcome to Module A!

- The competition has a fixed start and finish time. You must decide how to best divide your time.
- It is strongly recommended that you **read the entire Test Project before beginning any work,** so you understand the objectives and how the tasks relate to one another.

Documents/Files

This Test Project consists of the following documents/files:

- WSC2026_TP39_MA_actual_en.pdf
- WSC2026_TP39_MA_files.iso
    - prometheus.tar.gz — Official Prometheus v3.10.0 docker image
    - grafana.tar.gz — Official Grafana v12.4.2 docker image
    - dashboard.json — Sample Grafana Dashboard
    - index.php — Sample PHP page for the websites
    - recovery-commands.txt — Commands used by marking team to recover sha-gw-1

Logins

- Always choose the password: **Skill39@Shanghai**
- The **FTP / Mail / Web (apache2) / VPN** services must use the [username]@shenzhen.wsc login format, regardless of the authentication method.

Marking Notes

- Every node in the Test Project allows remote SSH using the root username and password. The marking team system needs root SSH access to all hosts to run the functional tests, verify configurations and inspect logs. Make sure you don't break/disable root SSH access on the nodes.
- The marking system uses **ICMP** to verify network reachability. Do not block ICMP by default.
- The Marking Team will not break or restart your configurations / services / virtual machines unless stated in the Test Project; however, they will actively interact with your services to evaluate them.
- The Test Project is designed to replicate industry best practices, requiring **centralized LDAPS authentication** and **a wildcard SSL/TLS certificate** to secure service communications.
    - Competitors who are unable to create a wildcard certificate can proceed with creating a normal certificate per service.
    - Competitors who are unable to configure secure services such as LDAPS, HTTPS, FTPS, SMTPS, IMAPS and syslog over mTLS can proceed with **plain LDAP**, **HTTP**, **FTP**, **SMTP**, **IMAP** and **TCP syslog** protocols.
    - Competitors who are unable to integrate with either LDAP or LDAPS can proceed with **local authentication**.
- Functional testing will be used to validate end-to-end configuration, and partial marks may be awarded when services are functional but insecure or using local authentication.
- To support testing and validation, the following tools are pre-installed on every node:
    - *curl* | *wget* | *dnsutils* | *ldap-utils* | *lftp* | *telnet* | *ssh* | *git* | *sshpass net-tools* | *traceroute* | *tcptraceroute* | *hping3* | *tcpdump* | *vim*
- All VMs are equipped with all Debian Blu-ray discs. This allows you to install software using apt.
- **sha-gw-1** comes preconfigured with basic IP addressing and network connectivity.
- **szx-srv-2** comes preconfigured with a **Git** service running at **http://192.168.10.11:8080**, using the credentials **gitadmin** / **Skill39@Shanghai**
- **szx-clt-1 and sha-clt-1 come pre-installed with the GNOME desktop environment and Visual Studio Code.**

© WorldSkills International

Description of project and tasks

You have just been hired as the sole IT administrator for **shenzhen.wsc**, a newly established company with a second site in **Shanghai**. The hardware has already been installed by one of the early staff members, so your role is to install, configure, and integrate all required services across both sites.

You will build the complete Linux-based network infrastructure, covering core network services, application services, security, and monitoring. You are expected to deliver a complete, working environment in which all services are properly integrated and accessible from the intended clients at both sites.

Default configurations should be used wherever specifics are not given.

The Test Project heavily emphasizes security best practices and end-to-end encrypted communication across all services (unless explicitly exempted). Manage your time wisely and **prioritize encryption**, **least privilege**, and **sensible defaults** wherever applicable.

© WorldSkills International

General Configuration

Clients and Servers

All Nodes	Local Users / Password	root & wsuser / Skill39@Shanghai
szx-gw-1	Hostname	szx-gw-1
	Domain Name	shenzhen.wsc
	DNS Server	192.168.20.10
	IP addresses	92.8.17.113/29 192.168.10.1/24 192.168.20.1/24 192.168.30.1/24
szx-srv-1	Hostname	szx-srv-1
	Domain Name	shenzhen.wsc
	DNS Server	192.168.20.10
	IP address	192.168.10.10/24
szx-srv-2	Hostname	szx-srv-2
	Domain Name	shenzhen.wsc
	DNS Server	192.168.20.10
	IP address	192.168.10.11/24
szx-srv-3	Hostname	szx-srv-3
	Domain Name	shenzhen.wsc
	DNS Server	127.0.0.1
	IP address	192.168.20.10/24
szx-clt-1	Hostname	szx-clt-1
	Domain Name	shenzhen.wsc
	DNS Server	DHCP (192.168.20.10)
	IP address	DHCP – SZX-CLIENT Network (192.168.30.100-199/24)
sha-gw-1	Hostname	sha-gw-1
	DNS Server	127.0.0.1
	IP addresses	92.8.17.114/29 192.168.1.1/24
sha-clt-1	Hostname	sha-clt-1
	DNS Server	192.168.1.1
	IP address	192.168.1.10/24

© WorldSkills International

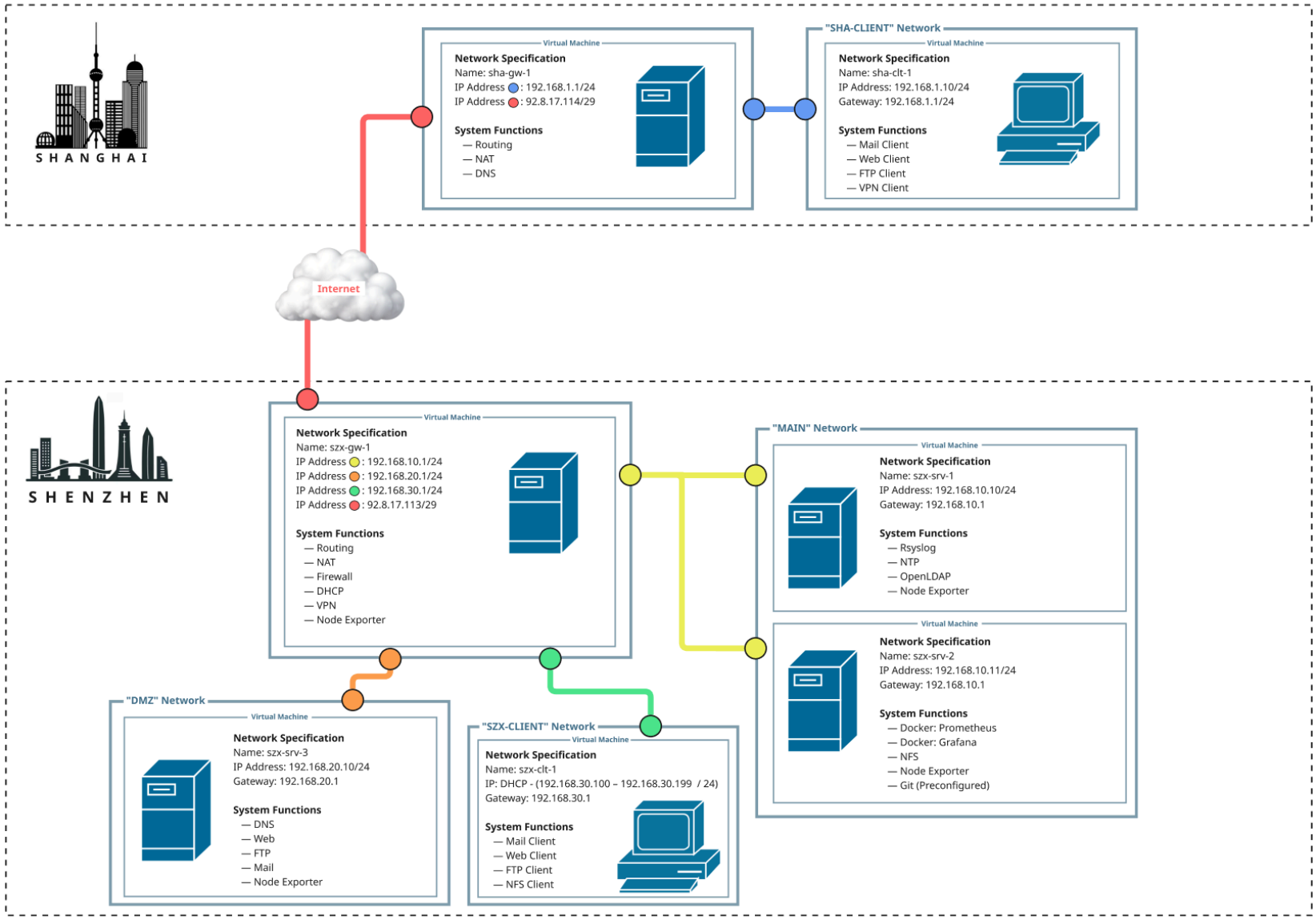
Network Specifications

SHA-CLIENT	Shanghai	192.168.1.0/24
Internet	Internet	92.8.17.112/29
MAIN	Shenzhen	192.168.10.0/24
DMZ	Shenzhen	192.168.20.0/24
SZX-CLIENT	Shenzhen	192.168.30.0/24

© WorldSkills International

Topology

Network Diagram: Module A - Linux Environment



© WorldSkills International

Part 1: Shenzhen Servers

Work Task: SSL/TLS Certificate

Throughout the Test Project, you may need to secure several services on different servers with SSL/TLS.

1. Generate a single self-signed **wildcard** certificate valid for **shenzhen.wsc** and all its subdomains (***.shenzhen.wsc**) with a one-year validity period.

   (a) For unspecified fields (e.g. CN, Country, ...) you may use any value.

2. Place the certificate files in the /etc/ssl/shenzhen directory on **szx-gw-1**.

   (a) The certificate files should be called **cert.pem** and **key.pem**

3. You can distribute these files to every server and use them for all services requiring SSL/TLS.

Work Task: Server szx-gw-1

Configure the server according to the specifications in the "Clients and Servers" table.

SSH

1. Make sure SSH listens on port 22 for all the Shenzhen network interfaces.
2. Make sure SSH listens on port 2222 for the Internet interface.

Routing / NAT / Firewall (nftables)

Note: You are **not** allowed to install iptables on this server.

1. Enable Routing.
2. Apply strict reverse-path filtering to all interfaces and enable martian packet logging.
3. Configure Source NAT to provide internet access for all Shenzhen network nodes.
4. Your ISP assigned an additional public IP prefix 188.20.21.0/24 to you. You decide to use it as NAT range for the DMZ network. Traffic originating from the DMZ to the internet must leave szx-gw-1 via the corresponding IP in this range and all incoming requests to 188.20.21.0/24 from the internet must be forwarded to the corresponding IP in the DMZ network.

   Example.1: Source 192.168.20.91 → Seen as 188.20.21.91 on the internet
   Example.2: Destination 188.20.21.137 → Forwarded to 192.168.20.137

5. Allow unidirectional access from SZX-CLIENT to DMZ and MAIN. The DMZ and MAIN networks should not be able to access SZX-CLIENT network.
6. Each IP Address can have only 5 simultaneous HTTP/HTTPS connections to szx-srv-3.
7. All inbound and outbound SMTP traffic (TCP/25) must be classified and forwarded with the highest network priority relative to other traffic.
8. To prevent any single client from monopolizing the bandwidth, the HTTP/HTTPS traffic from each SZX-CLIENT IP address must be rate-limited to a maximum of 2 Mbps.

DHCP (isc-dhcp-server)

1. Install and configure the DHCP server with the following specifications:

   (a) Range: 192.168.30.100 – 192.168.30.199 / 24
   (b) Gateway: 192.168.30.1
   (c) Primary DNS: 192.168.20.10
   (d) DNS-Suffix: shenzhen.wsc
   (e) Lease Duration: 90 minutes

VPN (openvpn)

1. Install and configure VPN server to accept VPN connections from internet and provide access to all Shenzhen network resources.
2. Use the address range 192.168.30.200 – 192.168.30.219 for VPN Clients.
3. Users should be authenticated against OpenLDAP over LDAPS, allowing only members of the "vpn" group to connect.

NTP Client (chrony)

1. Install and configure NTP client on this server to sync its time from szx-srv-1.

Node Exporter

1. Install Node Exporter (using apt) so that the Prometheus can scrape the server metrics.

Work Task: Server szx-srv-1

Configure the server according to the specifications in the "Clients and Servers" table.

NTP Server (chrony)

1. Install and configure the NTP server so that other servers can sync their time with this server.

Rsyslog

1. Securely collect logs from **szx-srv-3** server using **mutual TLS (mTLS) over TCP**, with x.509 certificate authentication on both server and client.
2. Store logs with the following formats:

   (a) Log Filename Format: /var/log/remote/[server-name].log
   (b) Log Content Format: [server-name] || [timestamp] || [log-message]
   Example:
   szx-srv-3 || Jul 8 02:02:40 || imuxsock: event socket log from systemd
   (c) Any log entry containing the string anomaly in the log content, should also be logged in /var/log/remote/anomalies.log file.

3. Logrotate

   (a) Compress all the collected log files daily.
   (b) Compressed files should be kept for 7 days and then be deleted from the server.

OpenLDAP (slapd)

1. Install and configure directory services for **shenzhen.wsc** domain.

(a) Use **Skill39@Shanghai** as the admin password and wherever required.

2. The OpenLDAP service should only serve **LDAPS** on the default port.
3. Create LDAP objects as indicated in the following tables:

(a) properly address the test project requirements.

ORGANIZATIONAL UNITS	LOCATION
people	Domain root
groups	Domain root
services	Domain root

USERS	LOCATION
user1	ou=people
user2	ou=people
user3	ou=people
user4	ou=people
user5	ou=people
user6	ou=people

GROUPS	LOCATION	MEMBERS
vpn	ou=groups	user1, user2
ftp	ou=groups	user3, user4
mail	ou=groups	user5, user6

Node Exporter

1. Install Node Exporter (using apt) so that the Prometheus can scrape the server metrics.

Work Task: Server szx-srv-2

Configure the server according to the specifications in the "Clients and Servers" table.

Monitoring Stack (Containerized)

1. Install Docker
2. Configure the monitoring stack components as containers on this server.

   (a) Prometheus:

   (i) Container Name: prometheus
   (ii) Container Image: Use the Prometheus docker image file provided in the ISO file.
   (iii) Port: 9090 (http)
   (iv) The Prometheus container's config file must be accessible and modifiable at /etc/prometheus/prometheus.yml on the host machine.

   (b) Grafana:

   (i) Container Name: grafana
   (ii) Container Image: Use the Grafana docker image file provided in the ISO file.
   (iii) Port: 3000 (http)

© WorldSkills International

(c) Every container must auto-restart on any failure and remain continuously available.

3. Prometheus (http://monitoring.shenzhen.wsc:9090)

   (a) Scrape all Shenzhen servers' node-exporter metrics, including the server itself.

4. Grafana (http://monitoring.shenzhen.wsc:3000)

   (a) Grafana login credentials should be: **admin / Skill39@Shanghai**
   (b) Add prometheus as a data source.
   (c) Import the dashboard.json provided in the ISO file into the dashboards.
   (d) Make sure the imported dashboard displays metrics from all Shenzhen servers.

Security Configuration

1. Protect the server against basic port-scanning attacks, especially scans that sweep across the entire port range.
2. Any source IP detected scanning the server must be automatically blocked for 5 minutes and then be automatically unblocked.

NFS

1. Install NFS server
2. Export /srv/fileshare via NFS and allow read-write access from the SZX-CLIENT network.

NTP Client (chrony)

1. Install and configure NTP client on this server to sync its time from szx-srv-1.

Node Exporter

2. Install Node Exporter (using apt) so that the Prometheus can scrape the server metrics.

Work Task: Server szx-srv-3

Configure the server according to the specifications in the "Clients and Servers" table.

Note: All services should be accessible from the internet via 188.20.21.10 address.

NTP Client (chrony)

1. Install and configure NTP client on this server to sync its time from szx-srv-1.

Rsyslog Client

1. All logs for this server should securely be sent to szx-srv-1 using mTLS.

Node Exporter

1. Install Node Exporter (using apt) so that the Prometheus can scrape the server metrics.

DNS (bind9)

2. Install bind9 DNS server.
3. Create a forward zone called **shenzhen.wsc**

   (a) Create the following A records with proper values:

- @ | internal (TTL: 6 Minutes)
- ntp | ftp | vpn | monitoring | git | fileshare | log | ldap | mail

   (b) Configure proper MX record for the mail server.

4. Requests from Internet for both websites should be resolved to the translated IP address of szx-srv-3 (188.20.21.10), but requests from the internal networks should be resolved to the untranslated IP address of szx-srv-3 (192.168.20.10).
5. Create a reverse lookup zone for **shenzhen.wsc**

   (a) Add PTR records pointing to the untranslated IPs for szx-srv-1, szx-srv-2, szx-srv-3

FTP (proftpd)

1. Install proftpd FTP server.
2. FTP connections must be secured with **explicit FTP over TLS (FTPS)** on the standard control **port 21**. Unencrypted (plaintext) FTP must be rejected.
3. Authenticate FTP users against OpenLDAP over LDAPS, allowing only members of the "ftp" group to connect.
4. Users' home directories should be /var/ftp/[username]@shenzhen.wsc
5. Users should be jailed into their home directories.

Web Server (apache2)

1. Create a virtual host for **shenzhen.wsc**

   (a) Create a 6MB file that is accessible at https://shenzhen.wsc/6mb.bin

      (i) This path will be used to evaluate your bandwidth shaping policy configured on szx-gw-1. Make sure you keep this file/path accessible so you don't lose marks.

   (b) All "pdf", "csv" and "docx" files should only be accessible from the SZX-CLIENT network.

2. Create a virtual host for **internal.shenzhen.wsc**

   (a) This virtual host should be protected by authentication.
   (b) All users defined in OpenLDAP (over LDAPS) should be able to authenticate and view the website contents.

3. Both websites must be accessible exclusively over an encrypted channel, and any plaintext request should be transparently upgraded so the user experience remains seamless.
4. Both websites should execute the provided index.php snippet and return the rendered HTML content to website visitors.

Mail Server

1. Set up mail service for shenzhen.wsc

   (a) Use **Postfix** as the **SMTP server** for mail transfer.
   (b) Use **Dovecot** as the **IMAP** server for mail retrieval.

2. Authenticate the mail users against OpenLDAP over LDAPS, allowing only members of the "mail" group to connect.
3. The SMTP submission service must be enabled on **TCP** port **587**, must require **STARTTLS**, and must only accept mail from authenticated users.
4. IMAP retrieval must be encrypted with **STARTTLS** on port **143** and must reject any unencrypted (plaintext) IMAP login.
5. The SMTP user-verification (VRFY) command must be disabled.
6. Each mailbox must be limited to 30 MB of storage.
7. If the SMTP server cannot deliver an email within 30 minutes, it should inform the sender about the delay.

© WorldSkills International

Part 2: Shanghai Servers

Work Task Server sha-gw-1

Configure the server according to the specifications in the "Clients and Servers" table.

Routing / NAT / Security Configuration

Note: The on-call team is trained exclusively on iptables, and all internal runbooks reference iptables commands. Use iptables for all related tasks on this server.

1. Enable routing.
2. Configure Source NAT to provide internet access for the SHA-CLIENT network.
3. To make basic remote OS fingerprinting more difficult, the ICMP responses from this server must appear to come from a Windows host.
4. Maximum ICMP packets from each IP address should be 5 packets in 25 seconds
5. Block anyone attempting SSH Bruteforce.

   (a) 5 failed login attempts within 30 seconds → connection timeout for 5 minutes.

6. Create a static route for 188.20.21.0/24 network using szx-gw-1 as the gateway.

DNS (bind9)

1. Install bind9 server
2. Configure standard forwarder to forward DNS queries to szx-srv-3

Ansible

1. To properly comply with modern disaster-recovery and business-continuity standards, this server needs to be fully recoverable using a single Ansible playbook. Write an Ansible playbook to fully address the requirements.
2. Your Ansible playbook and all the dependencies should be stored on the **main branch** of **shenzhen/disaster-recovery-iac** Git repository. Your playbook should fully recover / reinstall / reconfigure your setup on **sha-gw-1** in **a single run**, ideally written to remain idempotent, restoring the host to the exact working state you left it at the end of the Test Project.
3. The marking team will **revert** this server to its initial snapshot state and then run the commands in recovery-commands.txt from **szx-gw-1** to evaluate your work.

© WorldSkills International

Part 3: Clients

Work Task szx-clt-1

Configure the server according to the specifications in the "Clients and Servers" table.

FileZilla FTP Client

1. Install FileZilla FTP client
2. Log into the FTP server on szx-srv-3

   (a) Login as: user3@shenzhen.wsc
   (b) Upload a sample file named user3-upload.txt into your home directory (DO NOT DELETE!)

Thunderbird Mail Client

1. Install Thunderbird Mail Client
2. Configure the email client to connect to the mail server on szx-srv-3

   (a) Login as: user5@shenzhen.wsc
   (b) Send an email to user6@shenzhen.wsc (DO NOT DELETE!)

NFS Client

1. Mount the remote NFS share to the following local directory.

   (a) fileshare.shenzhen.wsc:/srv/fileshare ←→ /mnt/fileshare

2. Make sure the NFS mount is persisted properly in fstab and is accessible upon reboots.
3. Upload a sample file named nfs-upload.txt to the NFS mountpoint. (DO NOT DELETE!)

Work Task sha-clt-1

Configure the server according to the specifications in the "Clients and Servers" table.

FileZilla FTP Client

1. Install FileZilla FTP client
2. Log into the FTP server on szx-srv-3

   (a) Login as: user4@shenzhen.wsc
   (b) Upload a sample file named user4-upload.txt into your home directory (DO NOT DELETE!)

Thunderbird Mail Client

1. Install Thunderbird Mail Client
2. Configure the email client to connect to the mail server on szx-srv-3

   (a) Login as: user6@shenzhen.wsc
   (b) Send an email to user5@shenzhen.wsc (DO NOT DELETE!)

© WorldSkills International

OpenVPN Client

1. Install OpenVPN Client
2. Create a bash script in /opt/openvpn-client.sh
3. The script will be used to connect to the OpenVPN server (szx-gw-1)
4. After a successful VPN connection, you should be able to access all Shenzhen Internal Networks.
5. The script should have the following functionality

   (a) /opt/openvpn-client.sh -a connect -u <username> -p <password>
   Should connect to the VPN and then exit successfully and run in the background

   (b) /opt/openvpn-client.sh -a disconnect
   Should disconnect any background openvpn-client processes

   (c) /opt/openvpn-client.sh or /opt/openvpn-client.sh -h
   Should show script help

© WorldSkills International