T Level Technical Qualification in Digital Support Services

Employer set project (ESP)

Core skills

Cyber Security

Project brief – Task 1

v1.1: Specimen assessment materials
16 November 2023
603/6901/2

Internal reference: DSS-0001-04

T Level Technical Qualification in Digital Support Services Employer set project (ESP)

Core skills

Project brief

Firewall configuration

Contents

Student instructions

- read the project brief carefully before starting your work
- you must work independently and make your own decisions as to how to approach the tasks within the employer set project (ESP)
- you must clearly name and date all of the work that you produce during each supervised session
- you must hand over all of your work to your tutor at the end of each supervised session
- you must not work on the assessment in between supervised sessions

Student information

- the ESP will assess your knowledge, understanding and skills from across the core content of the qualification
- in order to achieve a grade for the core component, you must attempt both of the external examinations and the ESP
- the combined marks from these assessments will be aggregated to form the overall core component grade (A* to E and U) – if you do not attempt one of the assessments, or fail to reach the minimum standard across all assessments, you will receive a U grade
- the maximum time you will have to complete all tasks for the ESP is 12 hours 10 minutes:
    - your tutor will explain how this time is broken down per task and will confirm with you if individual tasks need to be completed across multiple sessions
    - at the end of each supervised session, your tutor will collect all ESP assessment materials before you leave the room
    - you must not take any assessment material outside of the room (for example, via a physical memory device)
    - you must not upload any work produced to any platform that will allow you to access materials outside of the supervised sessions (including email)
- you can fail to achieve marks if you do not fully meet the requirements of the task, or equally if you are not able to efficiently meet the requirements of the task
- the project is assessed out of a total of 76 marks (this includes 2 marks for your use of mathematics in task 3, and 4 marks for your use of English throughout tasks 2, 3 and 4) – the individual task marks are also shown throughout the project brief booklet at the start of each task

Plagiarism

Plagiarism may result in the external assessment task being awarded a U grade.

Presentation of work

- all of your work should be completed electronically using black font, Arial size 12pt unless otherwise specified
- any work not produced electronically must be agreed with your tutor, in which case the evidence you produce should be scanned and submitted as an electronic piece of evidence
- all your work should be clearly labelled with the relevant task number and your student details and be legible (for example, front page and headers)
- electronic files should be named using the following format – Surname_Initial_student number_evidence reference (for example, Smith_J_123456789_Task1) – for identification purposes; where evidence reference is shown, this should be replaced with the task number that the work reflects and saved as a .pdf format
- all pages of your work should be numbered in the format page X of Y, where X is the page number and Y is the total number of pages
- you must complete and sign the external assessment cover sheet (EACS) – declaration of authenticity form – and include it at the front of your assessment task evidence
- you must submit your evidence to the supervisor at the end of each session

Scenario

You are working as an infrastructure technician for Willow Technology.

The company has recently expanded at a rapid rate. As a result, the company has grown its staff from 25 to 50 and plans to continue expanding as their long-term aim is to have a workforce of around 200.

Some of its staff members work remotely, while the others are based in the single office unit that Willow Technology owns. Due to the nature of the business, staff require frequent access to shared files on the local area network (LAN).

As an infrastructure technician, you were required to implement a new company security system to prevent data loss and attacks. After you implemented a new firewall on your corporate network, a co-worker came to you and asked why they can no longer connect remotely to download files from the workplace. Additionally, some users have encountered problems connecting to the network during normal working hours (9am to 5pm).

Brief

As part of your role as an infrastructure technician, you are involved in a large security management project but have also been asked to support members of staff who require network support. Firstly, you should identify the cause of the problems raised by remote users and help them to resolve this.

Task 1: 2 hours 30 minutes

You must read the information on all pages provided for this task before starting your response.

(22 marks)

Scenario

Your line manager has asked you to investigate the problems the remote users are having. You have been provided with the following documents:

- control document A: network set-up and topology
- control document B: problems reported by users
- control document C: firewall policy

You are told that the connectivity problems do not affect all users and it is only users working remotely that have reported the issue.

Your line manager has asked you to review and ascertain the cause of the problems and undertake a fault-finding investigation to help resolve the issues. This investigation should analyse the initial issues and consider ways to resolve the problems. They have also asked you to create a test plan document that can be used by other team members to assist other users who encounter the same problem.

Instructions for students

Using the information provided above and in control documents A, B and C, you should investigate and identify the root cause of any network issue.

You should produce:

- your fault-finding investigation report (6 marks) which will include any recommended changes
- a test plan (16 marks) for use when troubleshooting network connectivity issues

Your test plan document should include:

- user details
- test dates
- computer specification and software
- proposed tests
- expected/actual outcomes of tests
- ability to record changes based on test outcomes
- record of your investigation leading to solution
- user acceptance of work completed

Evidence required for submission to NCFE

One document consisting of:

- your fault-finding investigation report
- your test plan document

When you have completed this task, you should save in a .pdf format and name your file:

- Surname_Initial_student number_evidence reference (for example, Smith_J_123456789_Task1)

Additional guidance

For this task, you will be issued with control documents A, B and C.

You will have access to a word processing application or other suitable software to enable you to complete this task.

Access to the internet is permitted.

Access to any online cloud storage is not permitted.

Use of online chat or email is not permitted.

Access to previous class notes/teaching materials is not permitted.

Control document A: network set-up and topology

Network set-up

Servers

Currently, Willow Technology maintains 2 servers located in a dedicated server room based at its head office in Winchester – one is to provide file and print services, the other is to add redundancy into the system. These servers were configured when the company started and have worked successfully for the last 2 years so have not been updated as to not affect their performance.

The current company network security policies have been in use for a long time and have not yet been updated to meet the growing size of the company. Whatever the outcome of this project, the business plans to install new servers and firewall. The company also plans to update its user permissions in the next 12 months.

Server specifications:

Server 1: file and print services

Server name: DC01

Operating system: Windows Server 2008 R2

Roles:

- file services
- print services
- domain name system (DNS)
- dynamic host configuration protocol (DHCP) – 30 users

Server 2: redundant server

Server name: FS01

Operating system: Windows Server 2008

Roles: redundancy

Previously, no remote access facilities were provided because there was no demand for remote working. A third server has recently been set up to support this. This new virtual private network (VPN) server has been set up at short notice and is running on a spare desktop PC from the office.

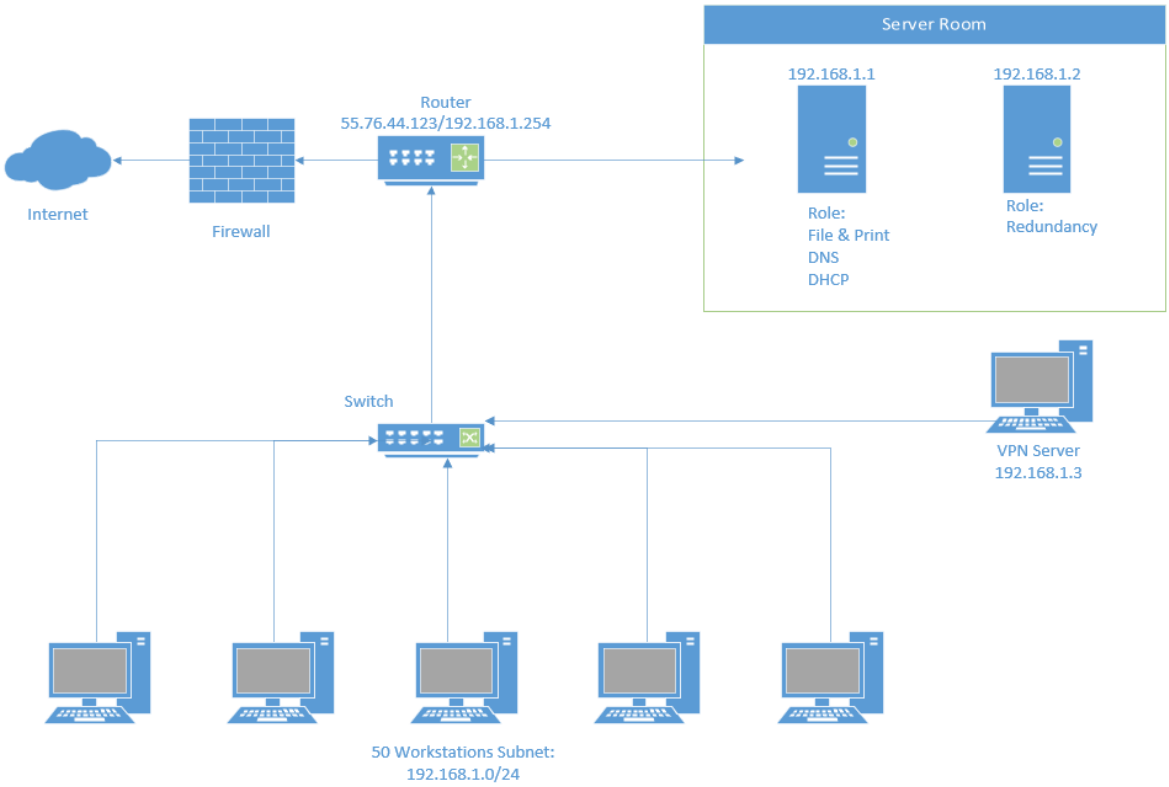
Server 3: VPN server

Server name: RAS01

Operating system: Windows Server 2019

Roles: VPN access

Network topology



Client PCs

Willow Technology has a workforce of 50 employees.

Staff working in the office use the desktop workstations provided for them. However, as the company also allows remote working, staff can work from home.

All client PCs are configured with anti-malware software (2019 edition). Scheduled updates to the operating system are on a quarterly basis, updates to anti-malware are monthly, and updates to application are not scheduled but reviewed on request.

Currently, all users have the same level of access so that all staff can access all resources.

Remote access

Staff working remotely are issued with a work laptop.

Staff induction

A set of videos, totalling 3 hours of training, is provided to staff as part of their induction, which introduces them to the network, software, systems and security. There are no requirements for staff to complete this again as the company feels that after staff have completed their probation, they will be confident in the company system and requirements.

Control document B: problems reported by users

User A – finance officer

User A – works remotely

User A – experiences problems accessing the company resources using the FTP server

User B – head of finance

User B – works both remotely and in the office

User B – experiences problems connecting to the company's FTP server when working from home but does not have any problems when working in the office

User C – sales representative

User C – works both remotely and in the office

User C – starts work later 2 days a week due to childcare issues, and on these days has experienced occasional problems connecting to the network when working remotely

Control document C: firewall policy

Firewall policy for Willow Technology

This firewall policy is expected to provide security functionality by enforcing intents on traffic that passes through our network devices. Traffic is permitted or denied based on the action defined as the firewall policy intent.

The firewall policy provides the following features:

- by default, all network traffic is permitted with rules in place to deny traffic if issues occur
- permits, rejects or denies traffic based on the application in use
- future consideration to identify not only hypertext transfer protocol (HTTP) but also any application running on top of it, enabling the company to properly enforce policies (for example, an application firewall intent could block HTTP traffic from Facebook but allow web access to HTTP traffic from Microsoft Outlook)

Table 1: the firewall policy protocol rules

Action	Service	Protocol	Source address	Destination address	Port
Allow	HTTP	TCP	192.168.1.0/24	Any	80
Allow	HTTPS	TCP	192.168.1.0/24	Any	443
Allow	POP3	TCP	192.168.1.0/24	Any	110
Allow	SMTP	TCP	192.168.1.0/24	Any	25
Allow	DHCP	UDP	192.168.1.0/24	192.168.1.1	67/68
Deny	SSH	TCP	192.168.1.0/24	Any	22
Deny	FTP	TCP	192.168.1.0/24	Any	21
Deny	SFTP	TCP	192.168.1.0/24	Any	22

Document information

The T Level Technical Qualification is a qualification approved and managed by the Institute for Apprenticeships and Technical Education. NCFE is currently authorised by the Institute to develop and deliver the T Level Technical Qualification in Digital Support Services.

Owner: Head of Assessment Design

Change History Record

Version	Description of change	Approval	Date of Issue
v1.0	Post approval, updated for publication		01 June 2023
v1.1	Sample added as a watermark	November 2023	16 November 2023