T Level Technical Qualification in Digital Support Services

Employer set project (ESP)

Core skills

Cyber Security

Project brief – Task 3

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

Internal reference: DSS-0001-08

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

Core skills

Project brief

Security management project proposal

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 the work that you produce during each supervised session
- you must hand over all 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
- to achieve a grade for the core component, you must attempt both 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 for which 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

Task 3: 4 hours

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

(24 marks)

Scenario

Following your meeting with the operations and IT manager, your line manager has provided you with a full specification of requirements and a network diagram (control document D). This document includes details of the current network and system security structure of the company, and the key results or outputs the company would like to achieve in the updated solution.

Your line manager has asked you to prepare a security management project proposal and an updated network topology diagram highlighting any security recommendations. You should use the project requirements in control document D, giving details of how you will provide security to the systems, servers and data protection to the company resources for all users.

Instructions for students

Your security management project proposal (24 marks) should include:

- an introduction outlining the current security issues
- a detailed overview of your plans, including:
  - how you will meet the project requirements outlined in control document D
  - how you will provide data protection and secured network connectivity for access to resources by all users
  - the equipment and network components you plan to use
  - how you plan to change from the current security set-up
- an updated network topology diagram of your proposed solution to accompany the proposal
- a justification of any equipment (hardware or software) or cloud services decisions you make
- estimated costs for any equipment (hardware or software) or cloud services recommended; your decisions should not only meet the brief but provide value for money (you should use the internet to research this)
- an explanation of any potential network and systems security issues with justification for recommended mitigations
- a final summary

When identifying costs, the company usually uses PC World Business and Dell as preferred suppliers. Where possible, these suppliers should be used for all equipment, tools or software recommendations before considering other suppliers. For cloud-based solutions, the company is extremely interested in solutions provided by Microsoft and Amazon Web Services but would consider other solutions if they were appropriate.

Evidence required for submission to NCFE

A document that contains:

- a detailed security management project proposal
- a detailed network topology diagram

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

- Surname_Initial_student number_evidence reference for example: Smith_J_123456789_Task3

Additional guidance

For this task you will be issued with control document D.

This task will also assess your English skills.

This task will also assess your mathematical skills, which are worth 2 marks.

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.

You are permitted to have up to a maximum of 15 minutes rest break during this task. This must be supervised.

Control document D: specification of requirements (to be issued at the start of task 3)

Network setup

Network, servers and firewalls

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 firewalls. 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 2008R2

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.

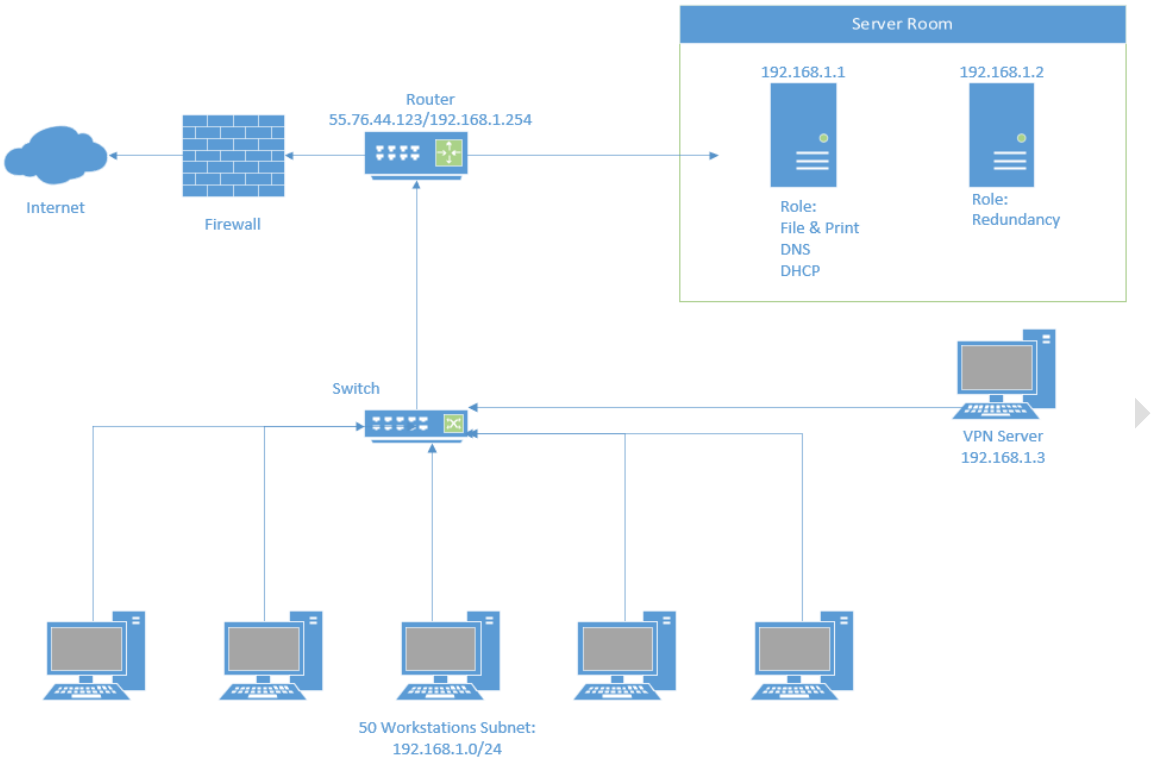
Server 3: VPN Server

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 applications 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.

Firewall policy for willows 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 by 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 HTTP (hypertext transfer protocol) 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

Project requirements

The senior management team are very keen to identify ways to use cloud resources to manage company computers. Therefore, assume that the current servers are due to be retired. Any solution you propose should either replace or remove the need to maintain the onsite servers.

Your solution should include:

- a robust solution for storing, managing and providing access to company files and data, regardless of location
- the ability to manage company computers and devices centrally
- a virtual desktop solution to allow secure access to data on personal equipment
- a solution that will allow staff to communicate and collaborate effectively with each other

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