

Portfolio (Part 1): CTF Marks : 18

Portfolio (Part 2): Analysis, Design, and Implementation of a Network Security Solution

Total Weight: 80% of the module

Total marks : 52/80

Marks for the Module: 70/100

How You Will Be Assessed

All marks for **Part 2** are awarded based on your:

- **PowerPoint presentation**
- **Live demonstration**
- **Responses to questions during the demo**

The **report is NOT marked**. It is used **only as evidence** of the practical work completed. Some tasks (e.g. installation) may be evidenced using screenshots and do **not** need to be demonstrated live.

Student Name	SAYEM AKTHER
Module name /Code	Enterprise Network Security ACCA7032
First Marker	Munya
Second Marker	

Generic Assessment Criteria	Marks Available	Marks awarded
1. Cognitive and Intellectual Skills – 5% (Security Thinking and Justification) This section assesses your ability to think critically about enterprise network security beyond the core implementation tasks. You will be assessed on your ability to:	5	3

Identify additional security features or controls that could further improve the security posture of the network Clearly explain why these features are appropriate in an enterprise environment Demonstrate awareness of security best practices, risks, and mitigation strategies NB: This section focuses on security reasoning and justification only		
2. Practical Application Skills – 50% This section assesses your ability to apply technical skills to secure an enterprise network using GAIA appliances. 2.1 GAIA Architecture and Deployment – 20% You will be assessed on: • Correct deployment and configuration of: ◦ A-GW ◦ A-SMS ◦ A-GUI • Appropriate IP addressing and user/profile configuration • Correct licensing of the Check Point Security Management Server • Successful connectivity between the Swansea Network and A-SMS Installation may be evidenced via screenshots and explained during the demo. You are not expected to reinstall or rebuild systems live. 2.2 Firewall Rules and Security Policies – 20% You will be assessed on: • Design and implementation of inbound and outbound firewall rules • Logical rule structure aligned with enterprise security best practices • Correct allowing and blocking of relevant services (e.g. ICMP, HTTP, FTP, SSH) • Clear explanation and validation of policy behaviour during the live demo	20 20 20	20 12

2.3 Additional Security Features – 10% <i>(Application to Your Network)</i> You will be assessed on how well you apply additional security concepts to your specific network design. You must: • Either: ◦ Implement additional security features where feasible, or ◦ Clearly map and justify proposed security features within your network • Clearly distinguish between: ◦ Implemented features, and ◦ Proposed (Not Implemented) features • Explain how these features integrate with: ◦ Existing firewall rules ◦ Network topology and traffic flows This section focuses on practical application and system-level understanding, not abstract ideas.	10	2
3. Transferable Skills for Life and Professional Practice – 25% This section assesses professional practice, communication, and demonstration skills during the live assessment. 3.1 Live Demonstration and Validation – 15% You will be assessed on: • Delivery of a clear and well-structured live demonstration • Effective use of the PowerPoint to support the demo • Appropriate judgement in deciding: ◦ What is demonstrated live, and ◦ What is evidenced via screenshots • Ability to validate configurations and security behaviour during the demo	15	10

3.2 Professional Communication and Responses to Questions – 10% You will be assessed on: • Clear, professional technical communication • Confidence and clarity when explaining configurations and decisions • Accurate and well-reasoned responses to questions • Ability to justify design and security choices under questioning Responses to questioning are used throughout the assessment to validate understanding.	10	5
Total	80	52

Feedback/Comments:

To score high marks, you were expected to deliver a well-structured live demonstration supported by PowerPoint, clearly explaining your GAIA architecture, IP addressing, licensing, and management connectivity. You were required to present a logically designed firewall policy following enterprise best practices, including correct rule ordering and the use of stealth and cleanup rules with appropriate service control. You should have validated your security behaviour using real traffic tests and logs, and clearly distinguished between implemented and proposed additional security features. Throughout the demo, you were expected to communicate professionally, justify your design decisions, and demonstrate sound security reasoning.

Your presentation appeared rushed and lacked a clear flow, which may have been affected by time management due to arriving close to your allocated slot. You implemented additional security features; however, these were not tested during the demo, and further proposed features could have been explained to strengthen your solution. You explained the concept of objects very well, but the architecture of the SMS and gateway was not clearly described, and you were unable to explain the difference between the cleanup and stealth rules or the principle of least-privilege policy. The live demonstration did not function as expected, which required additional questioning to assess your understanding; however, you did explain the challenges you faced and the solutions you applied clearly.