COLLEGE OF CREATIVE INNOVATION

Programme

Diploma in Cloud Computing and Cyber Security
(120 Credits)

Course

CCC603: Cyber Security in Cloud
(Level 6, 30 Credits, Version 1.1)

Assessment Title

Report and Proof of Concepts
(Network Security Expert using Fortinet)
CCC603 | Assessment-6
(Individual Assessment)

Weighting within the course

50%

Objective:

The purpose of this assessment is to design, implement, and document a secure hybrid cloud solution using FortiGate in AWS which ensures business continuity, compliance, and effective license management. Students will apply IT service management practices, develop procedures for distributing and monitoring cloud service licenses, and use automation tools to configure and manage secure cloud environments. Through both written reporting and practical demonstration, students will show their ability to plan, deploy, and automate IT infrastructure in line with organizational requirements and industry standards, while aligning with best practices for governance, security, and availability.

Course Learning Outcomes (LOs) covered:

LO3: Implement practices and processes to improve and support the delivery of IT service for business continuity, licensing and compliance with organizational requirements.
LO4: Develop procedures to distribute and manage the effective implementation of cloud service licenses within the organization.
LO5: Apply automation tools in the creation of applications, devices, and IT infrastructure within a secure cloud environment.

Qualification Graduate Profile Outcomes (GPOs) covered:

GPO1: Plan and use services, technologies, and tools to automate the deployment and management of devices, applications, and infrastructure by way of scripts to automate standard system procedures.

GPO4: Apply IT service management frameworks, change management processes and procedures to ensure licensing and compliance with organisational requirements, as well as concepts related to business continuity in an IT context.

Assessment Tasks to Learning Outcome and GPOs Mapping:

LO	GPO	Task	Task Component	Weighting
LO 3, LO 4	GPO4	Part A: Written Report	Executive Summary report	50%
LO5	GPO1	Part B: Proof of Concept	Practical Demonstration	50%
			Total	100%

Recommended Tasks Completion Timeline:

Full Time Week	Part Time	Progress	Submission
Week 21	Week 41,42	Start working on the Assessment	
Week 22	Week 43,44	Complete Task 1, Task 2	
Week 23	Week 45,46	Complete Task 3	
Week 24	Week 47,48	Complete Task 4 and submit	Assessment due by Week 24 (Full Time) Assessment due by Week 48 (Part Time)

Grading:

The final grade will be determined by the score achieved in this assessment based on the following table. Should a second or third attempt be required, the maximum contribution toward the overall mark for the tasks that required a second or third assessment attempt is 50%. **A late submission is considered a second attempt, so the contribution will be capped at 50%.**

To pass this assessment, you must meet the requirements of each of the learning outcomes (irrespective of the numerical grade awarded).

Grade	Range
A	Meet all course requirements, range (80—100%)
B	Meet all course requirements, range (65—79%)
C	Meet all course requirements, range (50—64%)
D	Did not meet all course requirements, range (40—49%)
E	Did not meet all course requirements, mark range (0—39%)

Candidate's Assessment Instructions:

- This assessment is an **open-book activity**; you can use your course and review notes, and offline or online resources, such as textbooks or online journals.
- You can always ask your online tutor if you need further explanation if the instructions are unclear.
- Your work should not be plagiarised. Plagiarism includes copying material without acknowledging it, copying from another student, getting another person to help you with your assessment, using material from commercial essays or assignment services, or using AI to create the answers.
- The purpose of this assessment is to assess your knowledge. In the event Yoobee suspects collusion, this will be addressed. For more information on plagiarism, please refer to the Student Handbook.
- Submit your completed assessment online in the correct space provided.
- Marks and feedback will be returned within **15 working days** of the submission date.
- By completing and submitting an assessment, you are authenticating that the work is original and does not violate plagiarism or copyright law. Authenticity is checked where any breaches of academic integrity are suspected. Please refer to the Student Handbook for further information.

Submission Instructions:

- Submit **one PDF** document **report** + **5–7-minute video walkthrough presentation in MP4 format as instructed in Part-B deliverables** to the LMS by the specified due date.

Your report should:

- Include your name and ID number
- Include the AWS account login details, a cover page, and a report index for verification purposes in your report.
- Use a standard citation format if external sources are referenced.
- Clearly label tasks and subtasks, and Diagrams must be clear and labeled properly.
- Include screenshots of each practical step in sequence, naming and numbering the screenshots. Screenshots must display the relevant settings or outputs for each step.
- Include your answers to the assessment questions for each task, describing choices, configurations, and learned insights with an appropriate practical and theoretical understanding.
- Submission must be in PDF format only because other formats may cause issues with accessing screenshots.

Assessment Tasks: Secure Cloud Service Implementation with Fortinet

Scenario:

Your organization is adopting a hybrid cloud strategy using AWS for business-critical workloads. IT leadership prioritizes **security, compliance, and licensing management** to maintain business continuity. You, as the Cloud Security Engineer, are tasked with:

- Designing a secure cloud network architecture using FortiGate firewalls in AWS.
- Developing procedures to manage cloud service licenses for security appliances.
- Using automation tools to configure FortiGate, route traffic, and enable continuity.
- Documenting all practices and controls in a professional report to demonstrate compliance with organizational and industry requirements.

Part A: Written Report (50%)

Objective: Executive Summary Report

Develop and document a secure hybrid cloud solution leveraging FortiGate in AWS, with emphasis on security, license management, regulatory compliance, and business continuity.

Your report must include below with word limit: 2,500–3,000 words (+/- 10%)

1. **Executive Summary**
    - Clear statement of the problem, objectives, and approach.
    - Summary of security, licensing, and continuity strategy.
2. **Cloud Security Architecture**
    - High-level network diagram of AWS VPC setup with FortiGate.
    - Description of FortiGate's role (firewalling, VPN termination, segmentation).
    - Explanation of routing, network segmentation, and policy enforcement.
3. **License Management Procedures**
    - Selection of BYOL (Bring Your Own License) or PAYG models for FortiGate.
    - Procedure for distributing and managing licenses in AWS.
    - Steps to monitor license expiration and compliance reporting.
4. **Compliance and Governance**
    - Identify key compliance frameworks (ISO 27001, CIS benchmarks, NIST CSF) relevant to cloud security.
    - Describe how FortiGate logging, reporting, and alerting support compliance.
    - Explain policy versioning and change documentation.
5. **Automation and Continuity Plan**
    - Describe scripts or CLI commands used to automate policy configuration, license activation, and backup.
    - High Availability (HA) setup for FortiGate (Active-Passive) with failover scenario.
    - Business continuity plan with RTO/RPO targets.
6. **Risk Assessment and Mitigation**
    - Identify potential misconfigurations, expired licenses, or downtime scenarios.
    - Propose mitigation strategies (monitoring, logging, scheduled health checks).
7. **Conclusion and Recommendations**
    - Reflect on lessons learned and propose future improvements (e.g., automation expansion, multi-AZ deployment).
8. **References**
    - Use APA referencing style for all sources, including Fortinet documentation, AWS guides, and any reference used.

Part B: Proof of Concepts (50%)

Objective: Practical Demonstration

This task focuses on designing, implementing, and verifying a secure and scalable AWS network architecture using a Virtual Private Cloud (VPC) and FortiGate firewall. You will demonstrate your ability to create a multi-subnet environment with proper routing, security configurations, and firewall deployment while adhering to AWS best practices for high availability and network segmentation. The exercise emphasizes hands-on cloud networking skills, including VPC customization, subnet planning, ENI management, and traffic verification through firewall rules.

The deliverable will validate your understanding of AWS networking concepts, routing strategies, multi-AZ deployment considerations, and firewall integration in a cloud environment.

1. Network Setup and VPC Design

- Delete default VPC in Sydney region.
- Create custom VPC Yourfirstname-VPC (10.160.0.0/16).
- Create Internet Gateway Yourfirstname_IGW and attach to VPC.

2. Subnet Creation

- LAN10 (10.160.10.0/24) – Public Subnet
- LAN20, LAN30 (10.160.20.0/24, 10.160.30.0/24) – Private Subnets (AZ a)
- LAN40, LAN50 (10.160.40.0/24, 10.160.50.0/24) – Private Subnets (AZ b, AZ c)

3. Route Tables

- Public_Route_Table (associate LAN10)
- Private_Route_Table (associate LAN20, LAN30, LAN40, LAN50)
- Set Private_Route_Table as main route table, delete default.

4. Security Group and ENIs

- Create Management_SG (allow all inbound initially).
- Create ENIs for LAN20–LAN50, assign private IPs.
- Disable Source/Dest check on ENIs.

5. FortiGate Deployment

- Launch FortiGate instance (t3. medium) from AWS Marketplace and automate this EC2 to start and stop using AWS Lambda function with appropriate security settings. **(Start time everyday 9:00 am and stop at 5:00 pm. NZT)**
- Attach ENIs LAN20 & LAN30 to FortiGate.
- Allocate and associate Elastic IP.
- Configure route tables (public via IGW, private via FortiGate ENI).

6. Firewall Verification

- Log in to FortiGate and change password.
- Ping test (e.g., exec ping 1.1.1.1).

Reflection Questions

- Why LAN40 and LAN50 cannot attach to the same FortiGate instance.
- Best practice for multi-AZ workloads.
- Diagram of final architecture.
- 5–7 min video walkthrough presentation in MP4 format.

Deliverables:
Screenshots of:

- VPC and subnets
- Route tables and associations
- Security Group rules
- ENI configurations
- FortiGate instance setup and ping test results
- Diagram of the final network architecture
- **5–7-minute video walkthrough presentation in MP4 format**

Marking Rubric

To pass this assessment, you must meet the requirements of each of the learning outcomes (irrespective of the numerical grade awarded).

Criterion		Evidence				
Task and Weightage		**A (80-100%)**	**B (65-79%)**	**C (50-64%)**	**D (40-49%)**	**E (0-39%**
Phase 1: (LO3, LO4, LO5) **Written Report** **(50%)**	**1.** Executive Summary **(5%)**	Clear problem statement, objectives, and strategic summary; professional, concise, insightful.	Clear but moderate depth; some details missing.	Vague or partial clarity; lacks insight.	Poorly articulated or missing.	Absent or completely unclear or Pending submission.
	2. Cloud Security/Architecture **(10%)**	High-quality diagrams; detailed FortiGate role explanation; strong understanding of routing, segmentation, and policies.	Diagrams adequate; explanation mostly clear but incomplete in places.	Basic diagrams; partial explanation; lacks depth.	Diagrams missing or incorrect; explanation unclear.	Minimal or no diagrams; explanation missing or Pending submission.
	3. License Management Procedures **(5%)**	Clear BYOL/PAYG rationale; detailed stepwise management; monitoring and compliance included.	Adequate explanation; minor missing details.	Basic procedure; monitoring/compliance weak.	Missing or incorrect procedures.	Largely missing or incorrect. or Pending submission.
	4. Compliance and Governance **(5%)**	Thorough compliance framework identification; links FortiGate logging/alerts to governance; policy versioning documented.	Frameworks identified; FortiGate compliance role explained partially.	Basic identification; weak explanation of compliance role.	Minimal or incorrect compliance discussion.	Largely missing or incorrect or Pending submission.
	5. Automation and Continuity Plan **(10%)**	Detailed automation scripts/CLI; HA Active-Passive; robust business continuity plan with clear RTO/RPO.	Automation and HA described continuity plan partially clear.	Basic automation/HA; continuity plan vague.	Automation, HA, continuity missing or inadequate.	Mostly missing or incorrect or Pending submission.
	6. Risk Assessment and Mitigation **(5%)**	Comprehensive risk identification; practical mitigation strategies; strong analytical thinking.	Risks identified; mitigation partially explained.	Basic risk identification; weak mitigation.	Risks and mitigation largely missing.	Minimal or absent risk discussion or Pending submission.
	7. Conclusion and Recommendations **(5%)**	Insightful reflection; practical, innovative recommendations.	Reflective; recommendations generic.	Minimal reflection; vague recommendations.	Conclusions unclear/missing, recommendations absent.	Absent or irrelevant or Pending submission.
	8. References and Professional Presentation **(5%)**	Accurate APA referencing; professionally structured; error-free; within word limit.	Mostly APA compliant; minor writing/format issues.	Incomplete/inconsistent references; some writing issues.	References missing/incorrect; poor structure/writing.	Largely missing / incorrect / Pending submission.

Criterion		Evidence				
Task and Weightage		**A (80-100%)**	**B (65-79%)**	**C (50-64%)**	**D (40-49%)**	**E (0-39%**
Phase 2: (LO3, LO4, LO5) **Proof of Concepts** **(50%)**	**1.** Network Setup and VPC Design. **(5%)**	Default VPC removed; custom VPC correctly created; IGW attached; naming conventions followed.	Minor errors in VPC or IGW setup; mostly correct naming.	VPC created but partial configuration; IGW missing or misconfigured.	VPC or IGW incorrectly configured, major errors.	VPC and IGW setup missing or incorrect
	2. Subnet Creation. **(5%)**	All subnets created accurately with correct CIDRs, AZ assignments, and public/private designation.	Minor errors in CIDRs, AZs, or subnet types.	Some subnets created; errors in addressing or placement.	Most subnets missing or misconfigured.	Subnets not created or entirely incorrect.
	3. Route Tables and Association. **(5%)**	Public and private route tables correctly created, associated, and main table set; default deleted.	Minor mistakes in associations or main table configuration.	Partial route table setup; some associations missing or incorrect.	Route tables mostly misconfigured or missing.	Route tables not created or incorrectly configured.
	4. Security Group and ENIs. **(5%)**	Security group created correctly; ENIs attached with correct private IPs; Source/Dest check disabled.	Minor errors in SG rules, ENIs, or configuration.	Partial SG/ENI setup; some settings incorrect.	Most SG/ENI configurations incorrect or missing.	SG/ENIs not created or entirely misconfigured.
	5. FortiGate Deployment. **(5%)**	FortiGate instance launched correctly; ENIs attached; EIP allocated; routing configured via FortiGate as required.	Minor mistakes in FortiGate setup, ENI attachment, or routing.	Partial FortiGate deployment; configuration issues present.	FortiGate setup largely incorrect or incomplete.	FortiGate instance missing or unusable.
	6. Firewall Verification and Testing. **(5%)**	FortiGate password changed; ping test successful; all verification steps completed.	Minor errors in verification; ping test partially successful.	Some verification performed; results incomplete.	Verification mostly missing or failed.	Verification not attempted or entirely incorrect.
	7. Architectural Diagram. **(5%)**	Accurate, professional diagram showing VPC, subnets, route tables, ENIs, FortiGate, and traffic flow.	Diagram mostly correct, minor omissions or labelling issues.	Basic diagram; some components missing or unclear.	Diagram incomplete or poorly presented.	Diagram missing or entirely incorrect.
	8. Reflection Questions. **(5%)**	Answers demonstrate deep understanding of multi-AZ limitations, best practices, and network design principles.	Answers mostly correct, minor gaps in reasoning.	Basic understanding; answers partially correct.	Answers weak or partially incorrect; lacks insight.	Answers missing or incorrect; no understanding demonstrated.
	9. Video Walkthrough Presentation. **(10%)**	5–7 min video clear, structured, professional; demonstrates all steps; effectively communicates and verified results.	Video mostly clear; minor omissions or presentation issues.	Video present; limited clarity or incomplete demonstration.	Video poorly presented, missing key steps or explanation	Video missing or fails to demonstrate task.