

Module: Enterprise Network Security

Module Code: ACCA7032

Submitted To:

Mr. Munyaradzi Murira

Lecturer

University of wales trinity saint david

Submitted By:

Sayem Akther Talukdar

Student ID: 2502919

University of wales trinity saint David

Submitted Date: 20-01-2026

Analysis and Implementation of Check Point GAIA Appliances (ACCA7032)

1 Purpose and Assessment Criteria

The **ACCA7032 Enterprise Network Security** module requires students to design, implement and justify a secure enterprise network using Check Point GAIA appliances. The Part 2 portfolio is assessed on three broad criteria:

1. **Cognitive and intellectual skills (5 %)** – Students must reason about additional security features beyond basic deployment, explain why the features are appropriate and demonstrate awareness of best practices.
2. **Practical application skills (50 %)** – The bulk of the marks are awarded for deploying and configuring the security gateway (A-GW), security management server (A-SMS) and GUI client (A-GUI), designing firewall policies and applying additional security features. Students must also ensure correct IP addressing and licensing of the management server, and prove connectivity between the Swansea network and A-SMS.
3. **Transferable skills (25 %)** – The live demonstration and PowerPoint presentation are assessed on clarity, structure and professional communication.

The written report is not marked but acts as evidence of the practical work. However, it is essential for documenting the configuration steps and rationale for the design decisions.

2 Lab Activity Sequence and Environment

The installation guide outlines a sequence of tasks. Students must deploy three GAIA appliances (A-GUI, A-SMS and A-GW), perform their initial configuration, interconnect the appliances with the existing S-DC/L-DC network and enforce security policies. A summary of the lab environment is shown in **Table 1**.

Table 1 – Summary of components and IP configuration

Component	Role	IP address(es) & network	Default gateway	Notes
A-GUI	SmartConsole client; GUI access	10.1.1.201/24	10.1.1.1	Windows 10 VM used to manage A-SMS and A-GW
A-SMS	Primary security management server	10.1.1.101/24	10.1.1.1	GAIA R81.20 (8 GB RAM, 25 GB HDD)
A-GW	Security gateway	Interfaces: 10.1.1.1/24, 192.168.1.254/24, 20.0.0.1/30	—	GAIA R81.20 (8 GB RAM, 25 GB HDD); acts as

Component	Role	IP address(es) & network	Default gateway	Notes
				firewall between networks
S-DC	Primary domain controller (SWANSEA.ACCA)	192.168.1.1/24	192.168.1.254	Pre-configured on host network
L-CD	Child domain controller (LONDON.SWANSEA.ACCA)	192.168.2.1/24, 20.0.0.2/30	—	Pre-configured; used for demonstration

The guide emphasizes that adapter settings must be correct and that a bridged adapter may be temporarily enabled on A-GUI to download the Smart Console installer and licenses.

3 Installation and Configuration

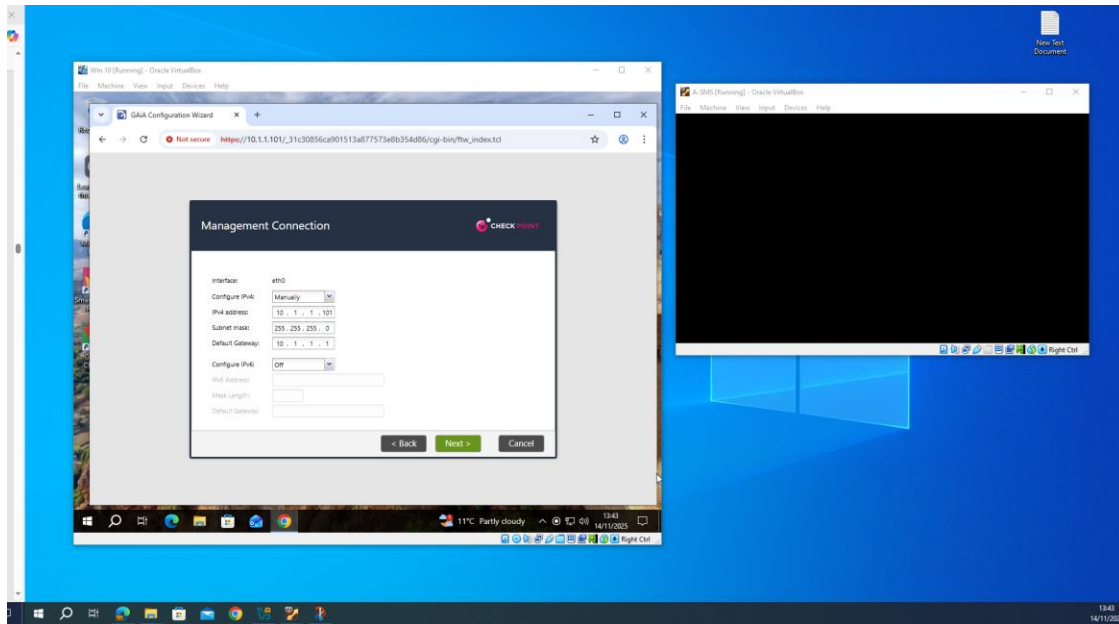
3.1 Installing the A-GUI (SmartConsole)

The A-GUI is a Windows 10 virtual machine used to run Check Point's Smart Console. The installation guide instructs students to download the Windows ISO and Smart Console package from the shared repository, install Windows, connect a bridged adapter to access the shared folder and install Smart Console. After installation, the Smart Console application (version R81.20) appears on the desktop.

3.2 Installing and Configuring the Security Management Server (A-SMS)

A-SMS is installed from the GAIA OS ISO. Key steps include selecting the correct OS type in VirtualBox, mounting the ISO and running the GAIA installer. During the first-time wizard, students must set the hostname (A-SMS), domain (swansea.acca) and DNS servers (192.168.1.1, 8.8.8.8, 4.2.2.2). Network Time Protocol (NTP) should be configured to time1.google.com and time2.google.com, with the timezone set to London/Europe. The product selection must enable **Security Management** and disable **Security Gateway**, defining the server as the *primary* management server. A new administrator (e.g., cpadmin/Chkp!234) is created for Smart Console access, and GUI clients are restricted to the 10.1.1.0/24 network. The wizard summary should list only *Security Management*.

After completing the wizard, the guide instructs students to run the api status command via the web terminal to ensure the management API is ready. The screenshot below shows the network configuration page of the A-SMS wizard, where the management IP address and default gateway are set.

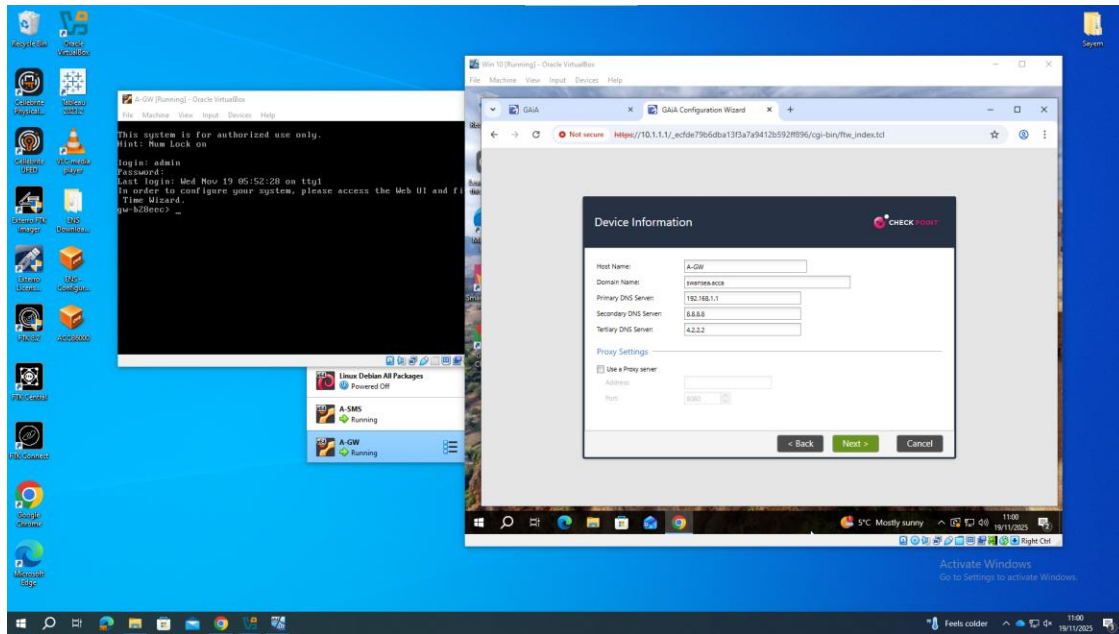


3.3 Installing and Configuring the Security Gateway (A-GW)

The A-GW is another GAIA OS installation. The installer sets the admin and maintenance passwords, and the first-time wizard configures the gateway as a **Security Gateway** (not management). The initial network interface (eth0) is assigned 10.1.1.1/24. After completing the wizard, students log into the GAIA web portal and edit each interface to match the lab network:

- **eth0** (Swansea) – 10.1.1.1/24.
- **eth1** (Internal SWA) – 192.168.1.254/24.
- **eth2** (External L-CD) – 20.0.0.1/30.
- **eth3** (External Internet) – obtain IP automatically.

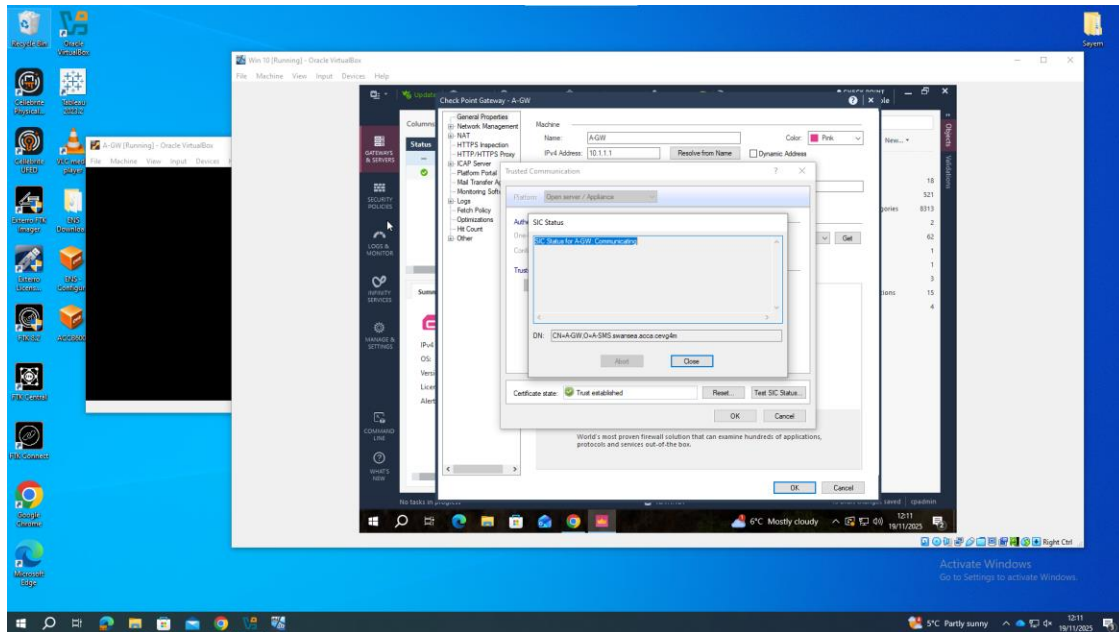
A screenshot of the GAIA network-interfaces page for A-GW is shown below. Note how each interface is labelled and configured with the correct subnet.



4 Establishing Secure Internal Communication and Licensing

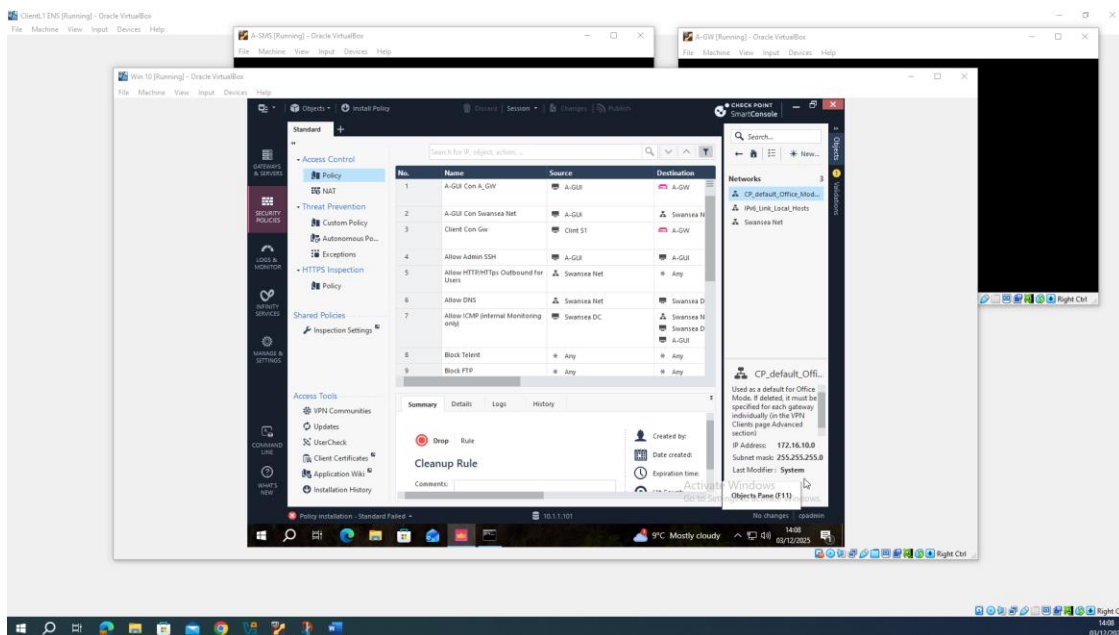
4.1 Creating the A-GW object and establishing SIC

After both appliances are configured, A-GW must be added as a gateway object in Smart Console. Students log into Smart Console on A-GUI using the A-SMS address (10.1.1.101) and credentials (cpadmin/Chkp!234). Using the Gateway Creation Wizard, they define an object named *A-GW*, specify its IP address and enter the one-time password (Chkp!234). When the topology information is retrieved, the gateway should match the configured interfaces; finishing the wizard adds the object and enables the firewall and monitoring blades. The guide instructs students to test **Secure Internal Communication (SIC)**. Selecting **Test SIC Status** should display a status of **Communicating**, indicating that the management server and gateway trust each other. This is shown in the screenshot below.



4.2 Managing Licenses via SmartUpdate

Licensing ensures that firewall and management blades remain active. The installation guide explains how to attach licenses to the appliances using the **SmartUpdate** utility. Students open the **Licence & Contracts** repository, add licences from file (e.g., A-SMS.lic and A-GW.lic) and attach them to the respective devices. The screenshot below shows the licence repository after a licence has been attached.



After attaching the licences and service contracts, the licence status for A-GW and A-SMS should read **Available** in the inventory. A licence report can be generated to confirm blade availability and expiration dates. For example, the provided report indicates that Firewall, Network Policy Management, Logging & Status and Monitoring are available for A-GW and A-SMS.

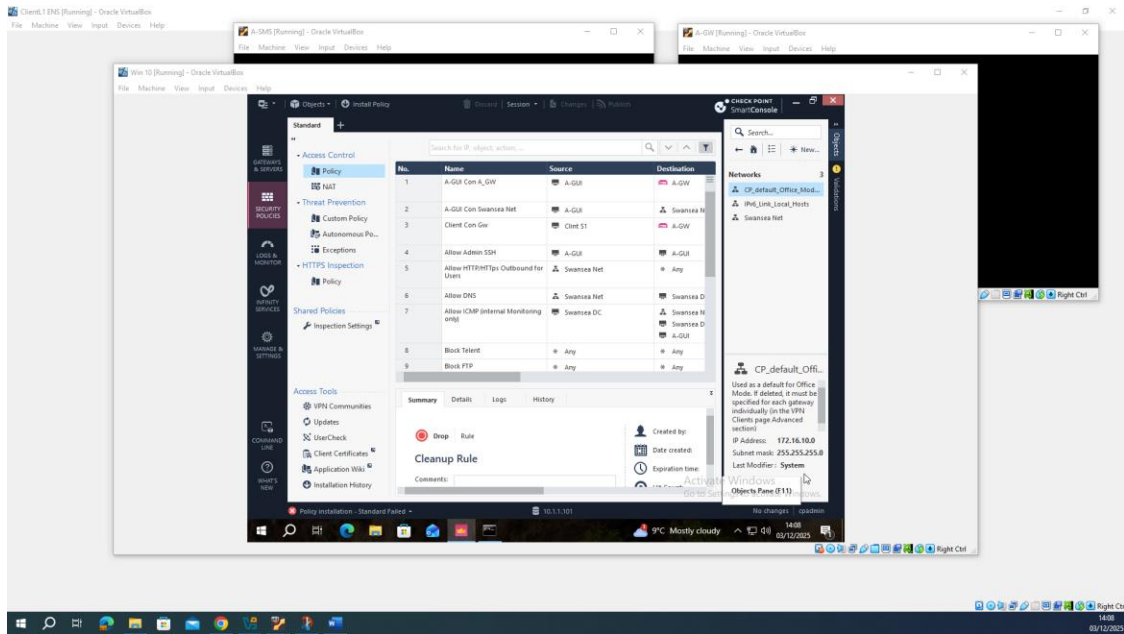
5 Firewall Policies and Threat Prevention

5.1 Designing Firewall Policies

The marking guide allocates 20 % of the practical marks to the design and implementation of firewall rules. Students are expected to create logical inbound and outbound policies that align with best practices and correctly allow or block services such as ICMP, HTTP, FTP and SSH. A recommended structure for this network includes:

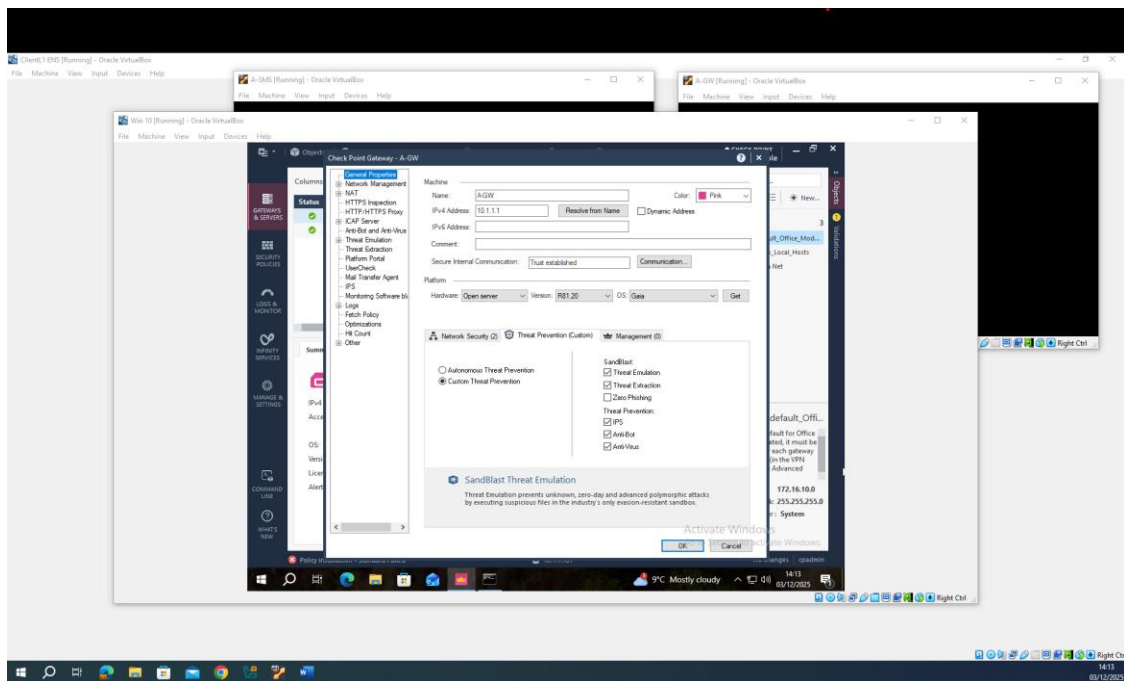
Rule	Source	Destination	Service	Action	Comment
1 (Stealth)	Any	A-GW	<i>Any</i>	Drop	Protects the gateway from direct access
2	A-GUI	A-SMS	HTTPS	Accept	Allows Smart Console management
3	A-SMS	A-GW	SIC	Accept	Allows management communication
4	Internal subnets (192.168.1.0/24)	Internet	HTTP/HTTPS/DNS	Accept	Allows web browsing & DNS
5	Internal subnets	External L-CD network (20.0.0.0/30)	RDP/DNS	Accept	Allows domain replication & remote admin
6	Any	Any	Any	Drop	Cleanup rule

A screenshot of the Smart Console policy editor illustrates the structure of these rules.



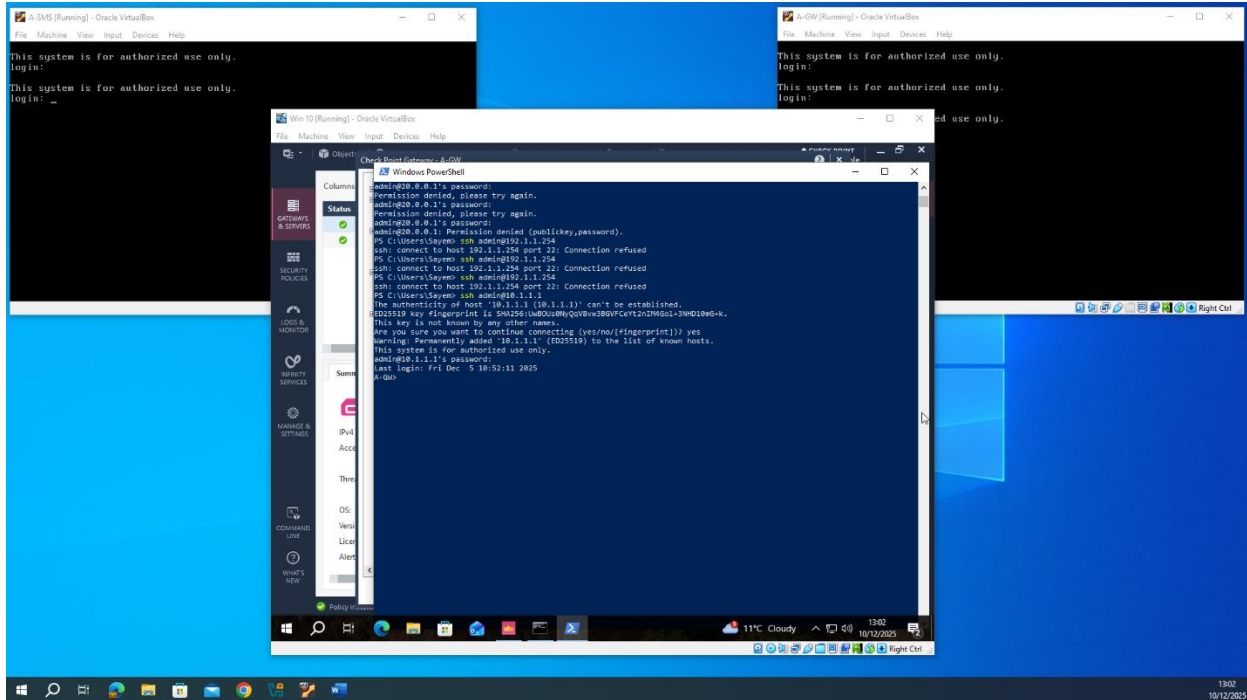
5.2 Enabling Threat-Prevention Features

Beyond basic firewalling, students are encouraged to enable additional blades such as **Intrusion Prevention (IPS)** and **Anti-Virus** on A-GW. The GAIA general properties page allows these blades to be enabled under the Threat Prevention section. The screenshot below shows IPS and Anti-Virus selected for activation.



5.3 Validating Connectivity and Policy Behaviour

After publishing the policy, network connectivity should be tested. Commands such as ping and ssh are used from A-GUI or S-DC to verify that permitted services succeed while blocked services fail. For instance, pings to 10.1.1.201 and 10.1.1.101 succeed whereas pings to an external address are dropped, demonstrating that the firewall behaves correctly. The screenshot below shows a sample ping test.



6 Results and Recommendations

6.1 Summary of Outcomes

Following the procedures above produced a functioning Check Point environment. A-GUI successfully installed Smart Console and connected to the management server. The A-SMS first-time wizard configured the device as the primary security management server with correct host and DNS settings. A-GW's network interfaces were configured to connect the Swansea network (10.1.1.0/24), the internal SWANSEA network (192.168.1.0/24), and the external link to the child domain (20.0.0.0/30). The Smart Console wizard created an A-GW object and established secure internal communication. Licences were attached to both appliances using SmartUpdate, and a licence inventory report confirmed that firewall, policy management, logging and monitoring blades were available. Firewall policies allowed necessary management and domain traffic while denying other traffic, and threat-prevention blades (IPS and Anti-Virus) were activated. Connectivity tests showed that permitted services functioned while prohibited traffic was blocked, demonstrating correct policy enforcement.

6.2 Proposed Security Enhancements

The marking guide encourages students to propose and justify additional security features. Based on industry best practices, the following enhancements are recommended:

- **Application Control & URL Filtering** – Implementing application control would allow fine-grained control over web and SaaS applications, preventing use of unauthorised apps. URL filtering can block access to malicious or inappropriate websites.
- **Anti-Bot & Threat Emulation** – Enabling these blades would detect and block command-and-control traffic and provide sandboxing of suspicious files, mitigating zero-day threats.
- **Identity Awareness** – Integrating the gateway with Active Directory would allow policies based on user or group rather than only IP, improving granularity.
- **VPN & Remote Access** – Configuring secure VPN tunnels would allow administrators to manage the network remotely without exposing management interfaces on the public Internet.
- **Centralised Logging & SIEM Integration** – Forwarding logs to an external SIEM or syslog server would provide better visibility and correlation of events across the environment.
- **Multi-factor Authentication (MFA)** – Adding MFA for administrative access to A-GUI and GAIA portals would reduce the risk of credential compromise.

Each proposed feature should be evaluated for feasibility within the lab environment and integrated with the existing policy framework.

7 Conclusion

This report documents the end-to-end deployment of a Check Point GAIA security solution for the ACCA7032 module. By following the installation guide, the A-GUI, A-SMS and A-GW appliances were deployed, configured and interconnected. Secure internal communication was established, licences were attached using SmartUpdate, firewall policies were implemented and threat-prevention blades were enabled. Evidence provided through screenshots and configuration summaries demonstrates that the environment meets the practical assessment criteria. Additional recommendations offer pathways to further strengthen the security posture. The accompanying slide deck summarises these activities and can be used as part of the live demonstration.