

ACCA7032 – Enterprise Network Security

Portfolio Part 2: Implementation Report

Student Name: Md Sadikur Rahman Chowdhury

Student ID: 2512666

Module: ACCA7032 Enterprise Network Security

1. Introduction

This report documents the complete setup and implementation of an enterprise firewall solution using Check Point GAiA R81.20. The implementation includes a Management Workstation (A-GUI), a Security Management Server (A-SMS), and a Security Gateway (A-GW). All configuration steps were performed manually and validated using real traffic tests. Screenshots are included in the relevant sections as evidence of the work completed.

2. A-GUI (Management Workstation) Setup

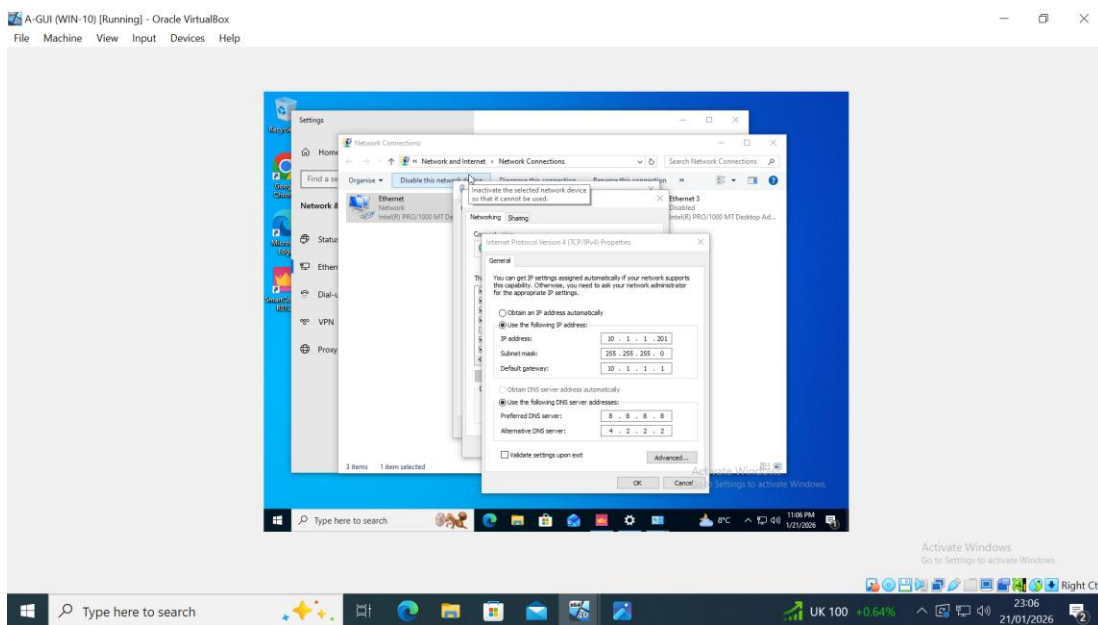
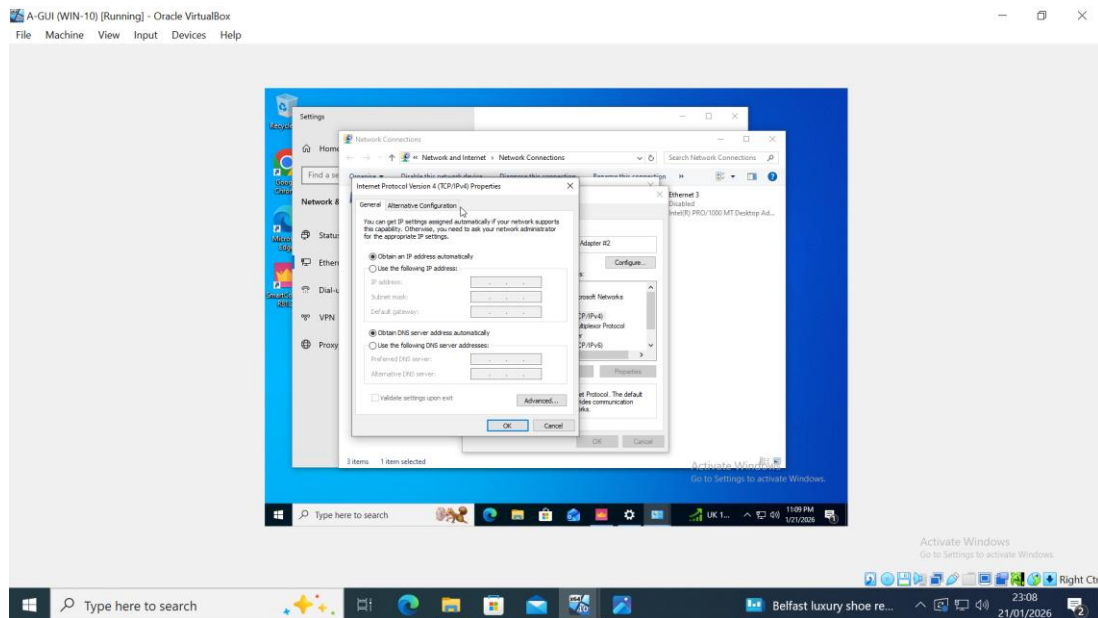
A Windows 10 virtual machine was deployed as the management workstation (A-GUI). This system was used to install SmartConsole and access the GAiA portals of both A-SMS and A-GW.

The network configuration of A-GUI was initially set to obtain an IP address automatically. It was later changed to a static configuration to ensure stable and predictable connectivity to the Check Point infrastructure.

Final configuration:

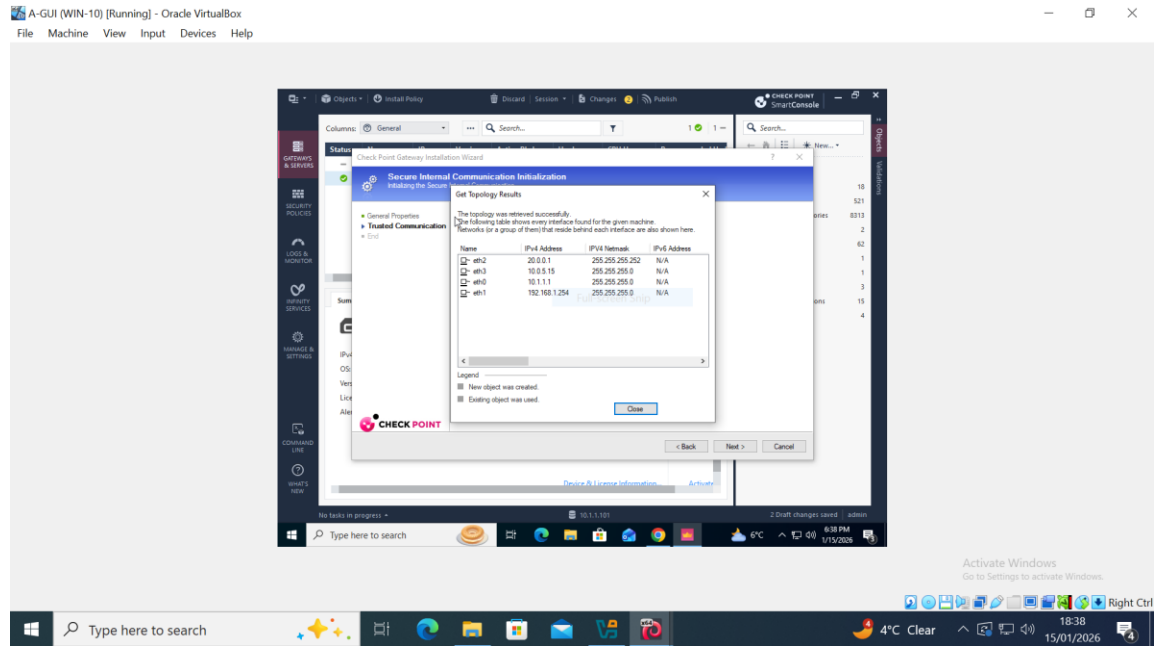
- IP Address: 10.1.1.201
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.1.1.1
- DNS Servers: 8.8.8.8, 4.2.2.2

Screenshot Evidence – A-GUI network configuration:



3. SmartConsole Installation

SmartConsole was installed on the A-GUI system. This tool was used to manage the Security Gateway, configure firewall policies, install policies, view logs, and manage licences.

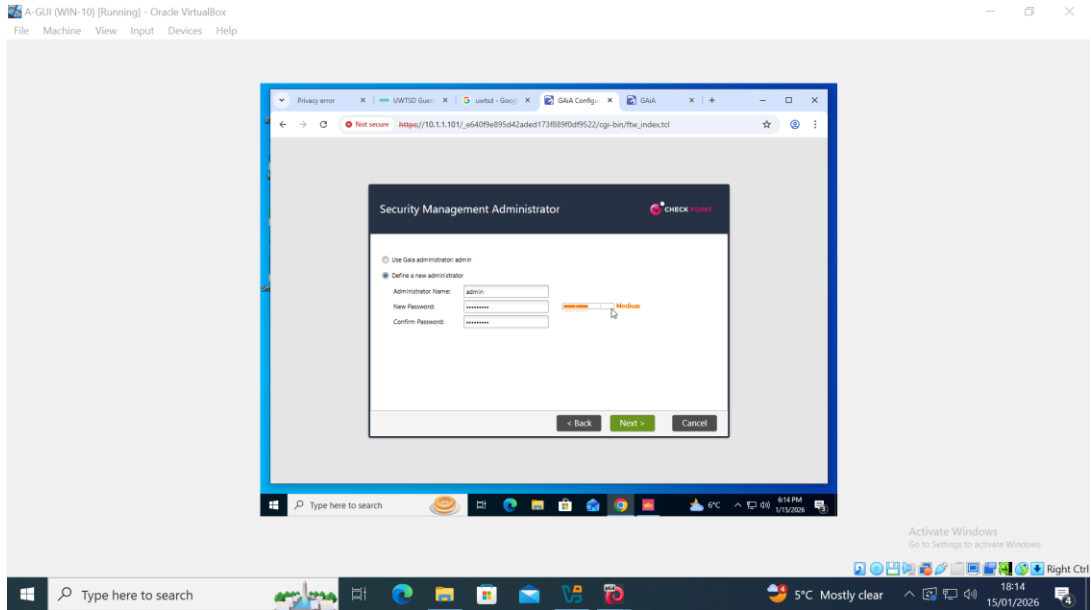


4. A-SMS (Security Management Server) Setup

The Security Management Server (A-SMS) was installed using Check Point GAiA R81.20. During the First Time Wizard, the server was configured as the Primary Security Management Server.

A-SMS Network Configuration:

- IP Address: 10.1.1.101
- Subnet Mask: 255.255.255.0
- Default Gateway: 10.1.1.1

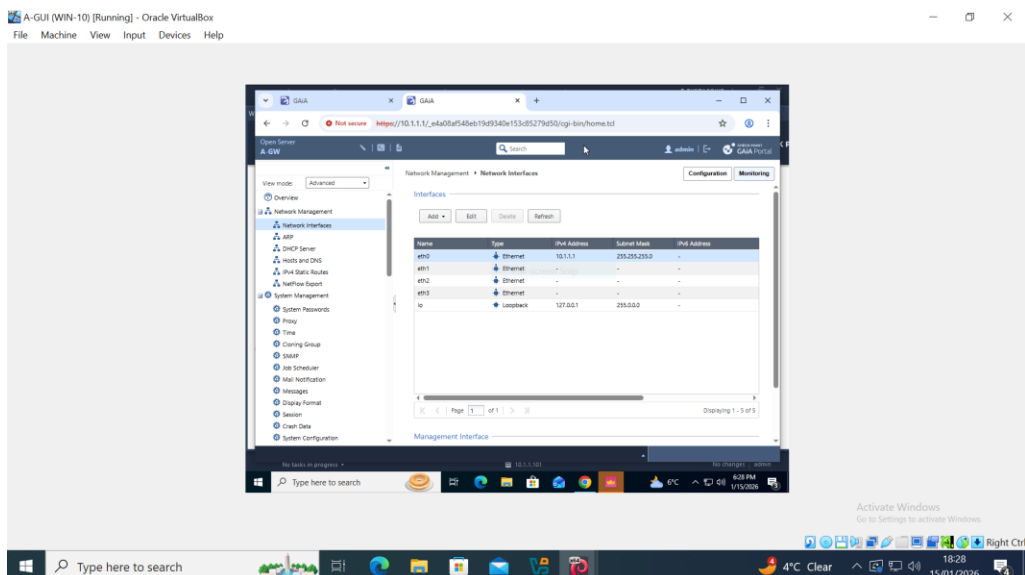


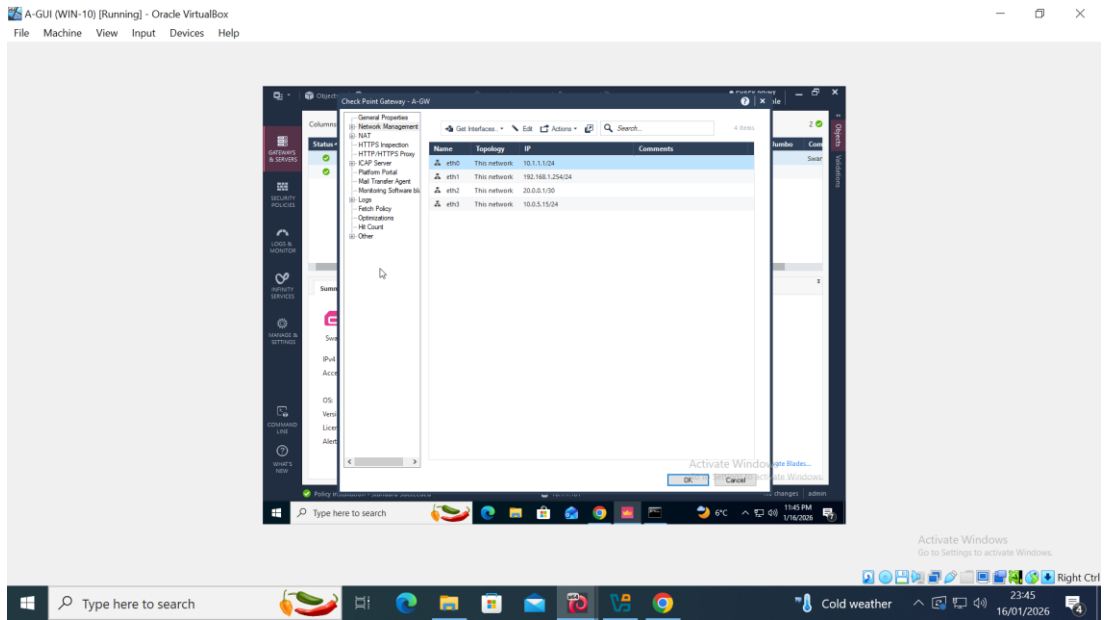
5. A-GW (Security Gateway) Setup

The Security Gateway (A-GW) was installed using GAIa R81.20 and configured with multiple interfaces to support management, internal, and external networks.

Configured Interfaces:

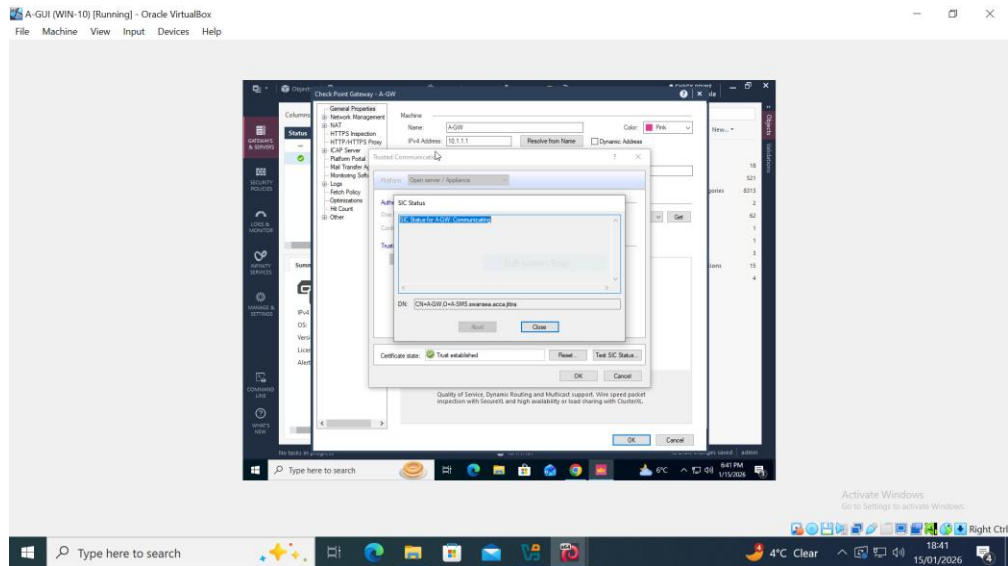
- eth0 – 10.1.1.1 (Management)
- eth1 – 192.168.1.254 (Internal)
- eth2 – 20.0.0.1 (WAN)
- eth3 – 10.0.5.15 (External)





6. Secure Internal Communication (SIC)

Secure Internal Communication (SIC) was established between A-SMS and A-GW using a one-time activation key. SIC status was verified and confirmed as Communicating.

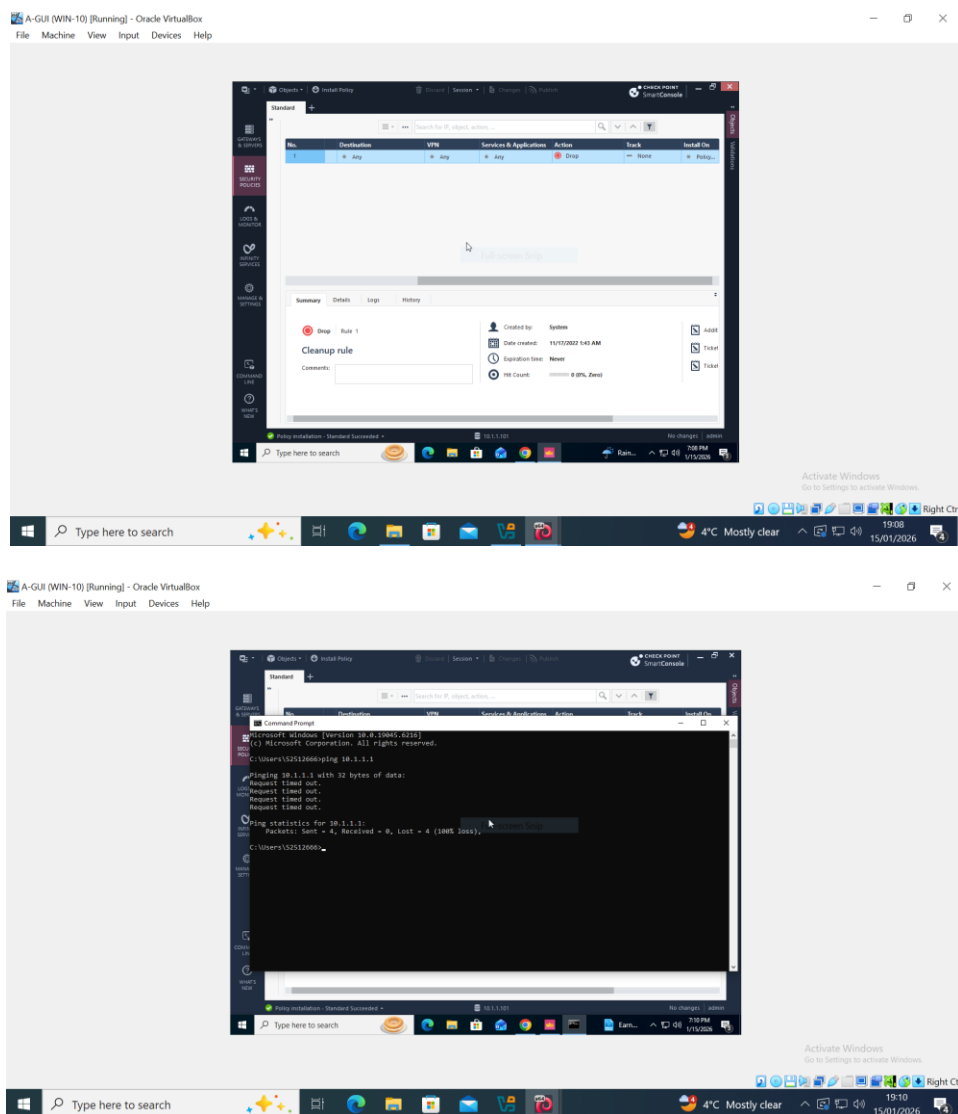


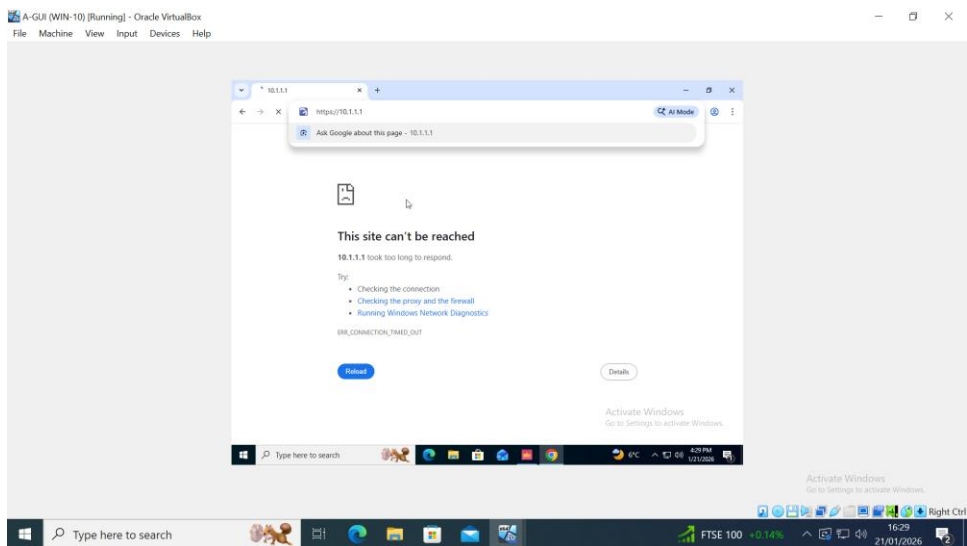
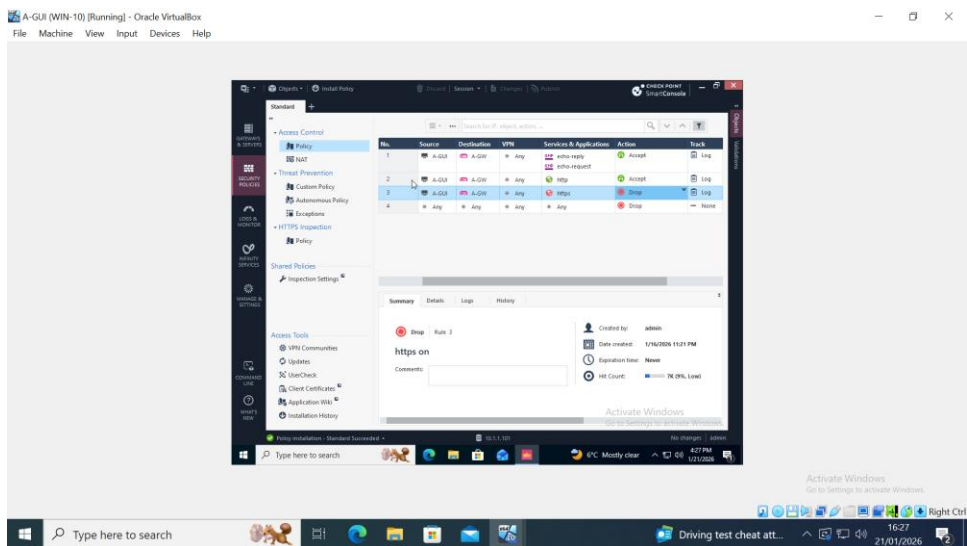
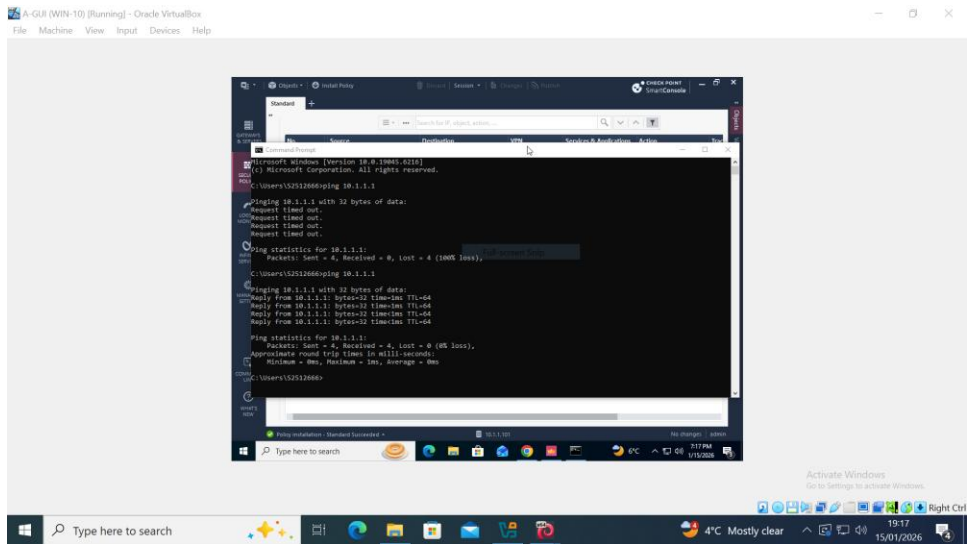
7. Firewall Policy Configuration and Testing

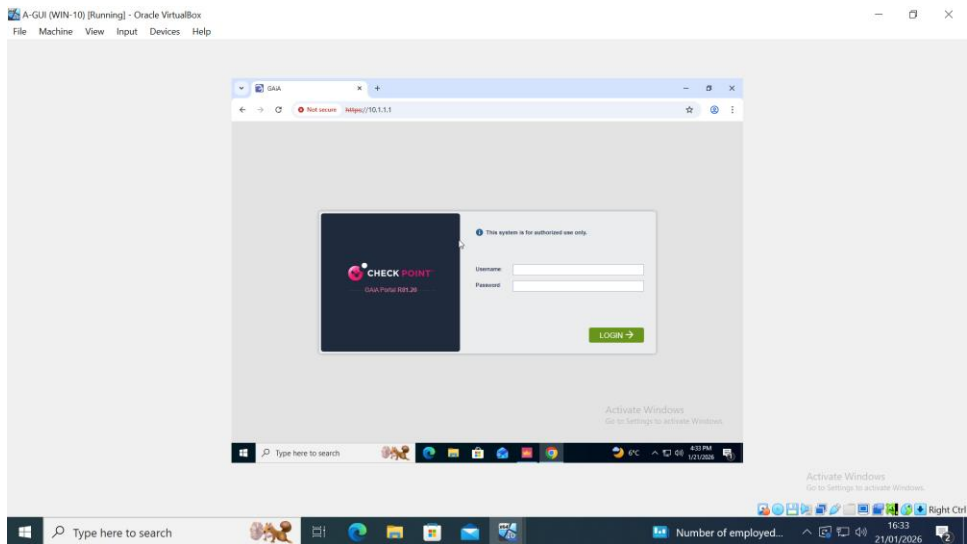
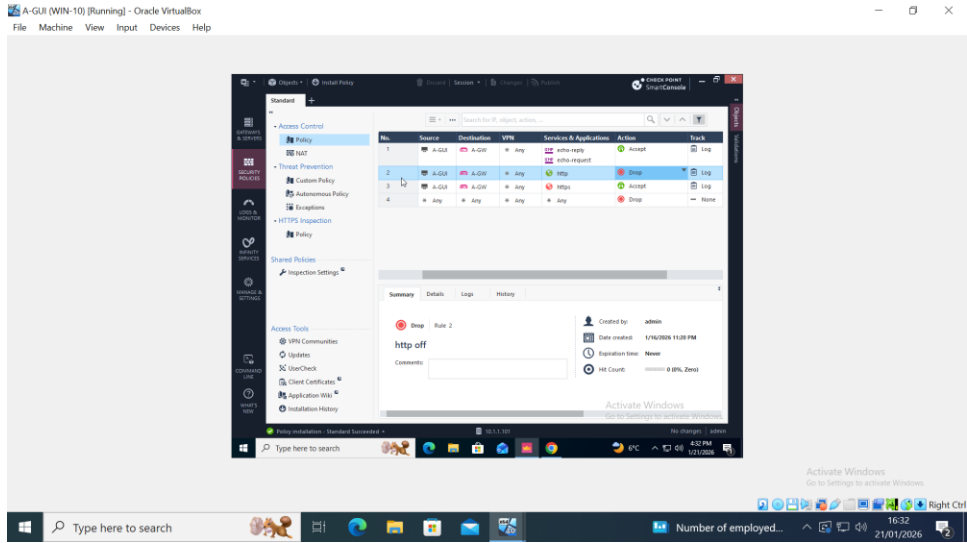
Firewall rules were created to control ICMP, HTTP, and HTTPS traffic. Policies were published and installed to the gateway.

Validation Tests:

- ICMP was blocked, then allowed to confirm rule enforcement
- HTTPS access was blocked and then allowed to prove policy behaviour

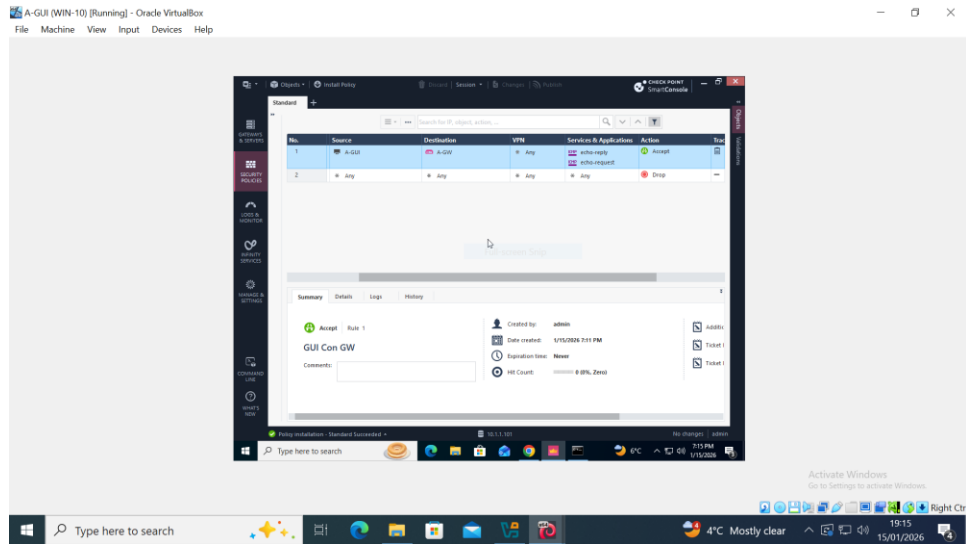
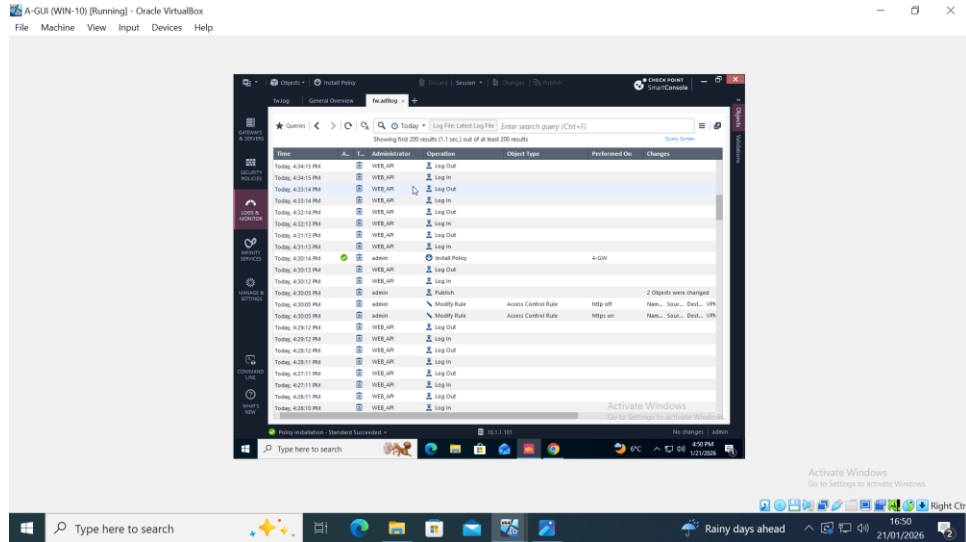






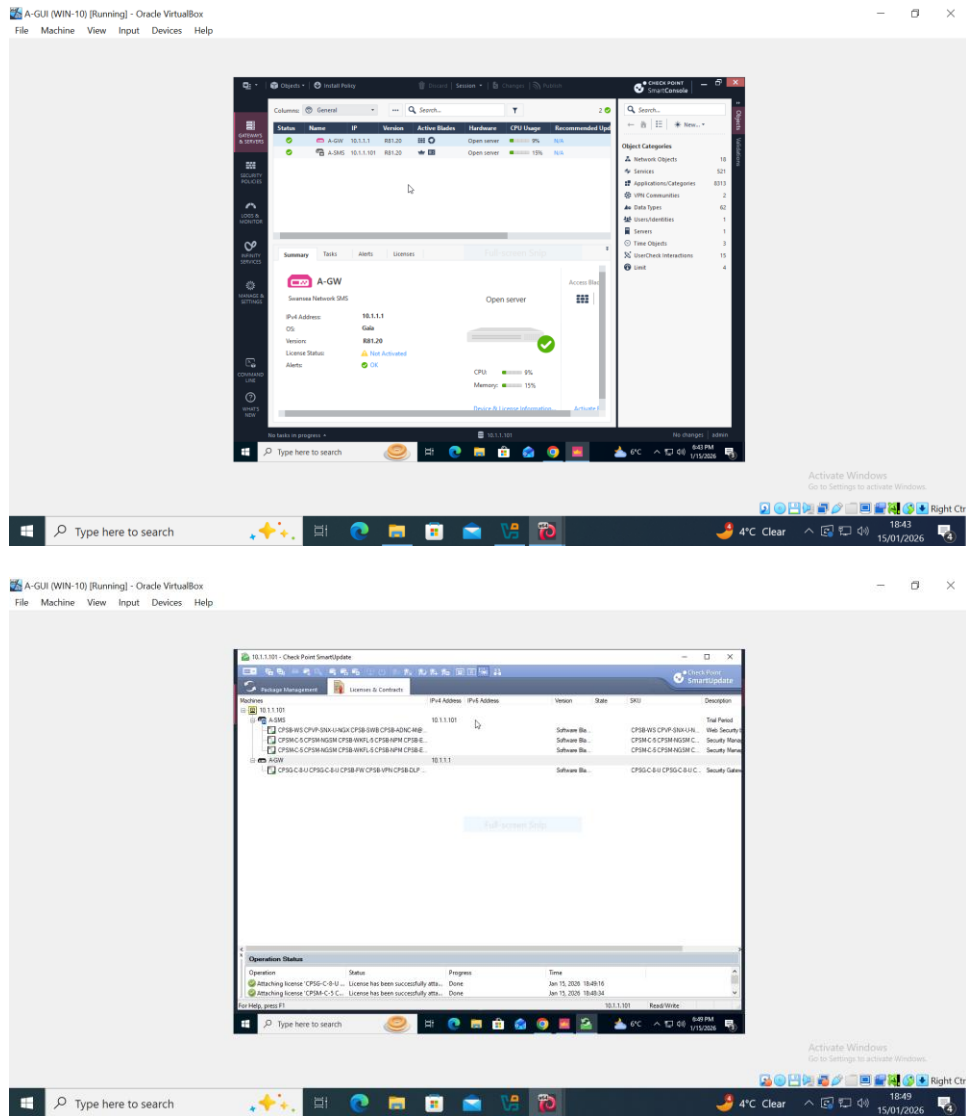
8. Logging and Monitoring

SmartConsole logs were reviewed to confirm policy installations, rule changes, and administrator activity.



9. Licence Management

Licences were attached to both A-SMS and A-GW using SmartUpdate. Licence status and inventory reports confirmed successful activation.



10. Conclusion

All components were successfully installed, configured, tested, and validated. The project demonstrates a complete enterprise firewall deployment using Check Point GAIa with centralised management, secure communication, policy enforcement, logging, and licensing.