Implementation of a Network Security Solution

Student Name: Md Hasibul Islam

Student ID: 2421865

Lecturer: Renuga Jayakumar

Module: Enterprise Network Security

Module code: ACCA7032

University of Wales Trinity Saint David (UWTSD)

Submission Date: 12th August 2026

Table of Contents

Part 2 - Securing the Enterprise Network 3
1. Introduction 3
1.1 Summary of Completion Status 3
2. Network Topology 4
3. SMS Deployment, SmartConsole & Licensing 5
3.1 SmartConsole Installation & SMS Connectivity 5
3.2 Gateway & Management Server Status 5
3.3 Licensing Verification 7
3.4 Connectivity Verification 8
4. Firewall Rule Base & Traffic Control 11
4.1 Access Control Policy 11
4.2 Traffic Logging & Verification 12
5. Conclusion 13
7. Attachment 13

Part 2 - Securing the Enterprise Network

1. Introduction

This report documents Part 2 of the enterprise network security implementation, building on the baseline deployment completed in Part One. The objective of this stage is to secure the enterprise network using Check Point Gaia appliances: deploying a centralised Security Management Server (SMS), enforcing an Access Control rule base that reflects real-world enterprise policy, and applying further hardening measures aligned with industry practice.

The report is structured around the three graded components of the Part 2 brief — Security Management Server deployment and licensing (30%), firewall policy and traffic control (30%), and additional security enhancements (20%) — with supporting screenshot evidence captured directly from the lab environment for each completed configuration.

1.1 Summary of Completion Status

Task	Weight	Status	Evidenced in
1. SMS deployment, SmartConsole & licensing	30%	Complete	Section 3
2. Firewall rule base & traffic control	30%	Core rules complete; IPS/anti-malware blocked by expired evaluation licences (§3.3); identity awareness pending	Section 4
3. Additional security enhancements	20%	Pending	Section 5

Table 1: *Summary of completion status by task.*

2. Network Topology

Figure 1 shows the target topology for Part 2, as provided in the assignment brief. A-GW acts as the perimeter security gateway, mediating traffic between the Internet, the core management segment (A-GUI and A-SMS, 10.1.1.0/24), and two further internal domains reachable via the gateway's IntSWA and ExtLCD interfaces.

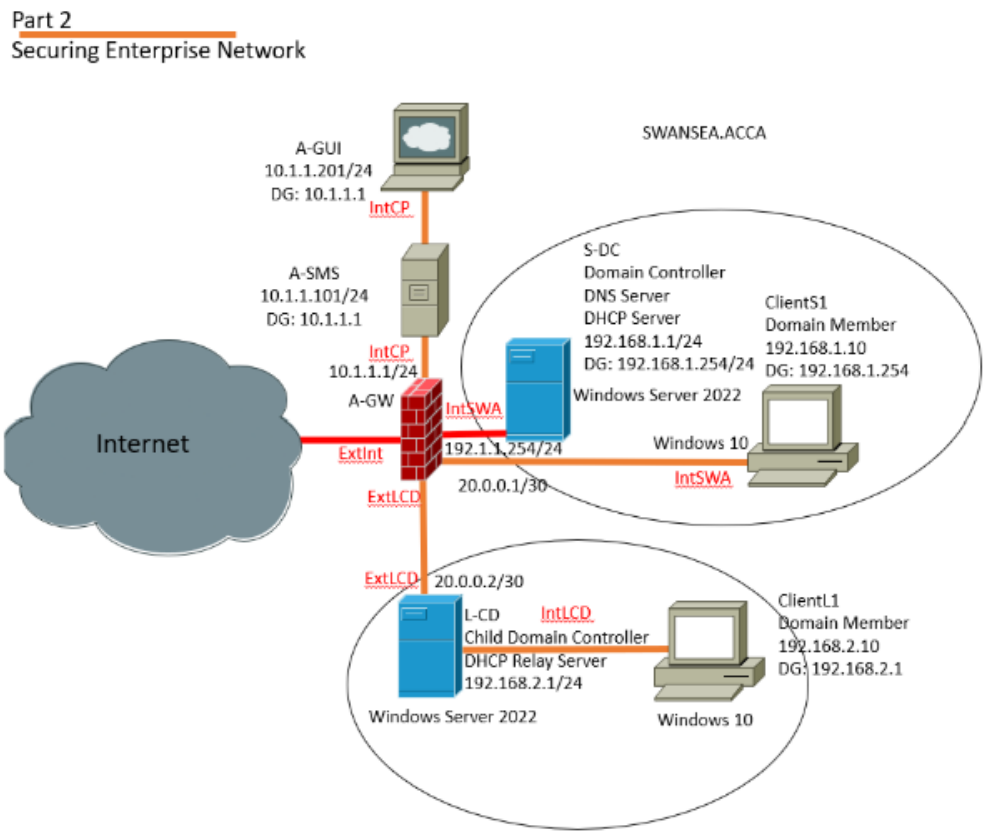

Figure 1: Target topology for Part 2 — Securing Enterprise Network, as provided in the assignment brief.

The evidence captured for this report covers the core management segment — A-GW (10.1.1.1), A-SMS (10.1.1.101) and A-GUI (10.1.1.201) — where the Security Management Server was deployed, licensed, and used to build and test the Access Control policy. Configuration of the wider domain-controller segments (S-DC and L-CD) shown in Figure 1 is not evidenced in the current screenshot set and is noted as outstanding in Section 5.

3. SMS Deployment, SmartConsole & Licensing

3.1 SmartConsole Installation & SMS Connectivity

SmartConsole was installed on the A-GUI management workstation and used to connect to the Security Management Server at 10.1.1.101 (A-SMS), authenticating as user “hasib”. This confirms SmartConsole is correctly installed and able to reach the SMS over the management network.

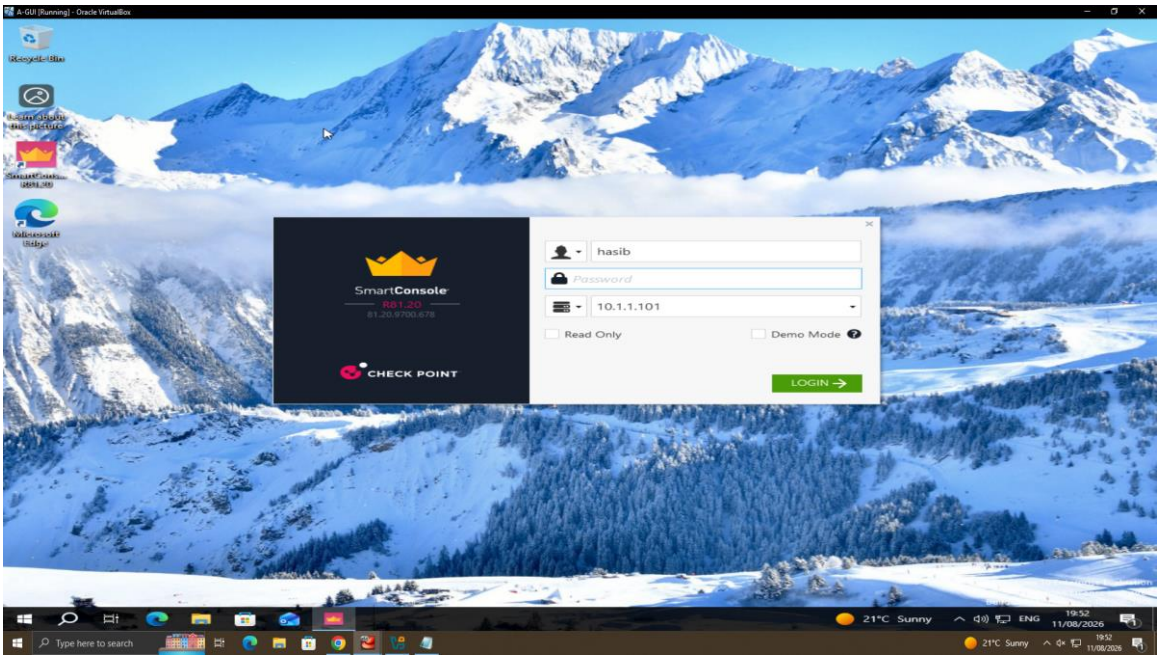

Figure 2: SmartConsole login prompt on A-GUI, connecting to the Security Management Server at 10.1.1.101.

3.2 Gateway & Management Server Status

Once connected, the Gateways & Servers view confirms both managed objects are reachable and healthy: A-GW (10.1.1.1) and A-SMS (10.1.1.101), both running Gaia R81.20 on an Open Server platform, shown with a green OK status. The A-SMS summary panel confirms its Network Policy Management and Logging & Status blades are active, with license status OK.

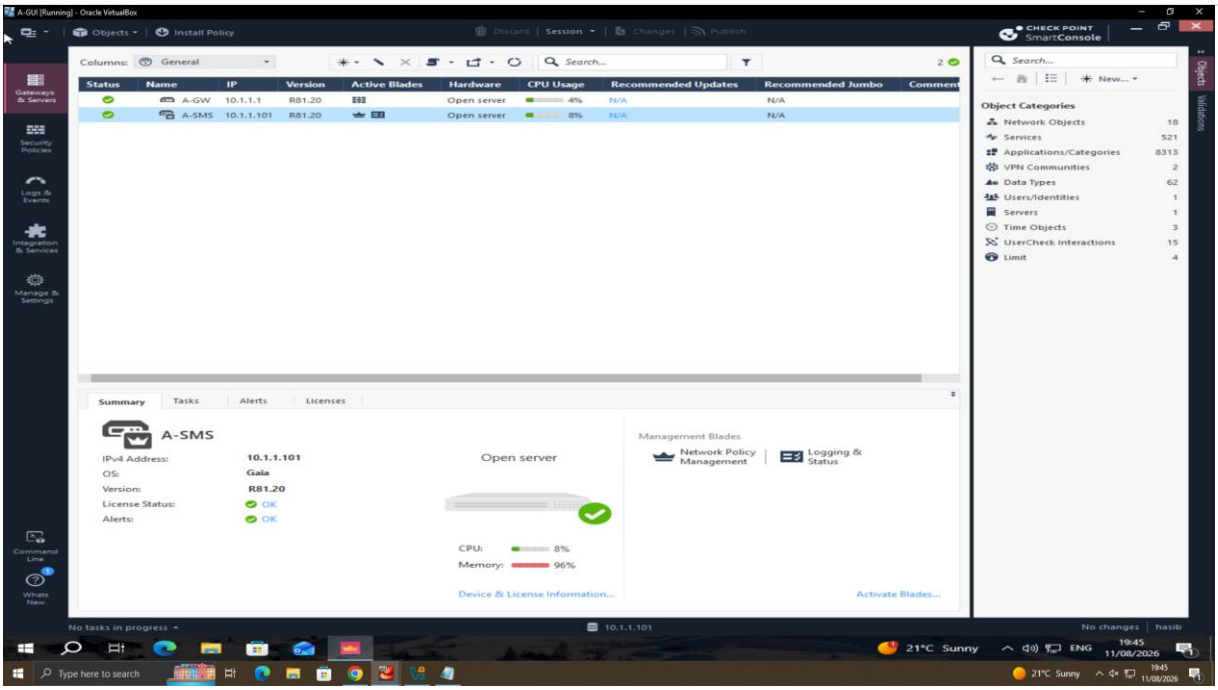

Figure 3: SmartConsole Gateways & Servers view, showing A-GW and A-SMS status with the A-SMS summary panel (license status OK).

It is noted that the A-SMS summary panel records memory utilisation of 96% at the time of capture, while CPU load remained low (8%). CPU headroom is healthy, but sustained high memory usage on the management server is worth monitoring going forward, as it can affect SmartConsole responsiveness and log indexing performance under heavier load.

The gateway's own summary panel (Figure 4) independently confirms A-GW: Access Control Policy “Standard” installed 11/08/2026 19:44, running Gaia R81.20, License Status OK, with the Firewall access blade active and comfortable headroom on both CPU (4%) and memory (41%).

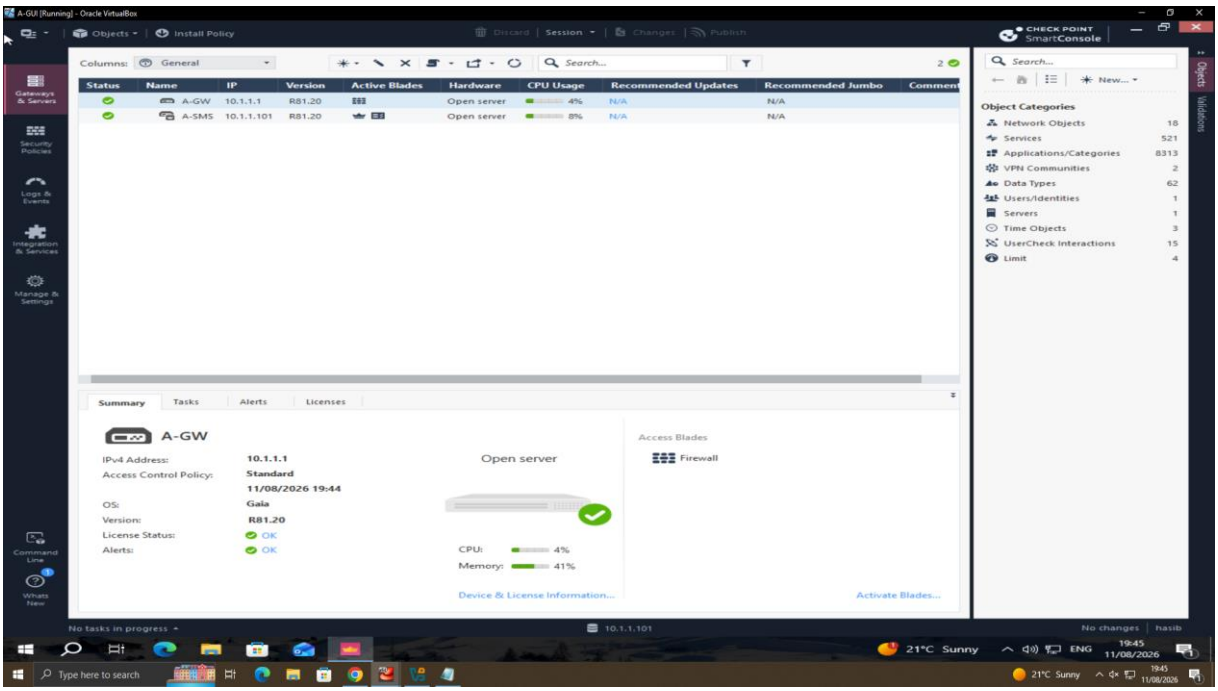

Figure 4: SmartConsole Gateways & Servers — A-GW summary panel, confirming policy installation time, license status and blade activation.

3.3 Licensing Verification

License and contract status for both the management server and the gateway were verified using SmartUpdate's Licenses & Contracts view. Table 2 summarises the primary licence entries attached to each machine.

Machine	SKU	Description	Expiration	Has Contract
A-GW (10.1.1.1)	CPSG-C-8-U…	Security Gateway Container for Security Gateway…	21 Sep 2026	Yes
A-SMS (10.1.1.101)	CPSB-WS CPVP-SNX-U-N…	Web Security blade / SSL Network Extender for u…	21 Sep 2026	Yes
A-SMS (10.1.1.101)	CPSM-C-5 CPSM-NGSM C…	Security Management container to manage up to …	never	Yes
A-SMS (10.1.1.101)	CPSM-C-5 CPSM-NGSM C…	Security Management container to manage up to …	never	Yes
A-SMS (10.1.1.101)	CPSM-C-5 CPSM-NGSM C…	Security Management container to manage up to …	never	Yes

Table 2: *Primary licence entries for A-GW and A-SMS, transcribed from SmartUpdate (Figure 5).*

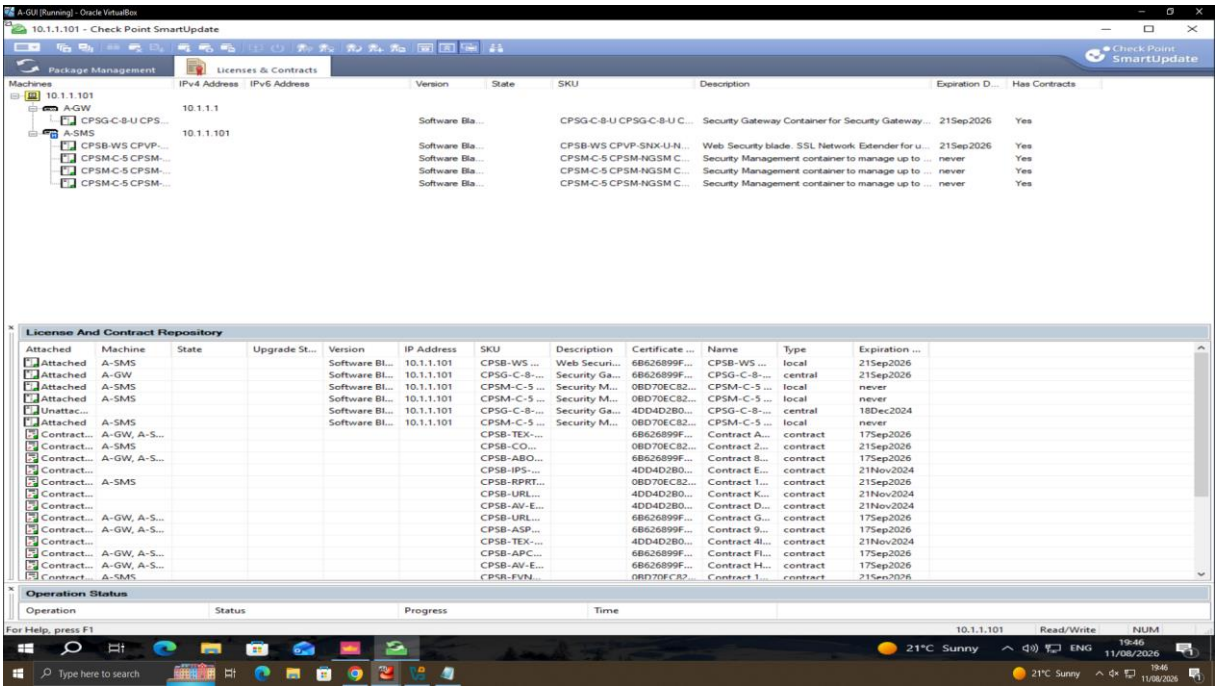

Figure 5: *SmartUpdate — Licenses & Contracts view for A-GW and A-SMS, including the full License and Contract Repository.*

The License and Contract Repository (lower pane of Figure 5) also lists several older contract records with expiration dates in late 2024 (e.g. 21 Nov 2024, 18 Dec 2024) that had already lapsed by the time of testing in August 2026. These correspond to legacy or unattached entries rather than the primary active licences summarised in Table 2, but the distinction between current in-date licences and legacy contract history is worth carrying into the final report so licence compliance is not overstated.

SmartUpdate's own License/Contract Expiration dialog (Figure 6) confirms this directly and names the specific SKUs involved: the CPSG-C-8-U package licence expired 18 December 2024, and a cluster of evaluation contracts — CPSB-IPS-EVAL, CPSB-URLF-EVAL, CPSB-AV-EVAL, CPSB-TEX-EVAL,

CPSB-ASPM-EVAL and CPSB-TE-EVAL — all expired together on 21 November 2024. This is directly relevant to the Task 2 added-advantage items discussed in Section 4.3: the evaluation licences that would cover IPS, Anti-Virus and related blades have already lapsed, so a renewed or replacement licence is a prerequisite for enabling them, not just a configuration step.

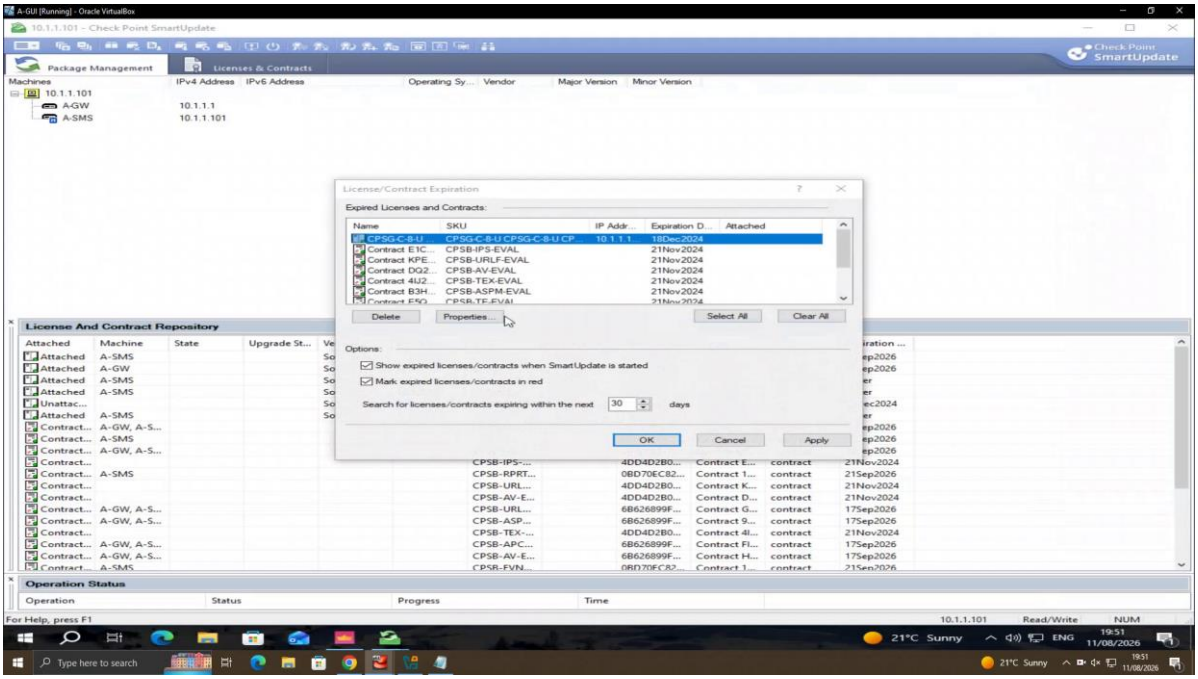

Figure 6: SmartUpdate — License/Contract Expiration dialog, listing the expired package licence and evaluation contracts (IPS, URL Filtering, Anti-Virus, and related blades).

3.4 Connectivity Verification

End-to-end reachability between the management server and gateway was tested from the Gaia CLI on both ends. From A-GW, a 15-packet ping to A-SMS (10.1.1.101) completed with 0% packet loss and an average round-trip time of 0.445 ms, confirming the management channel is up.

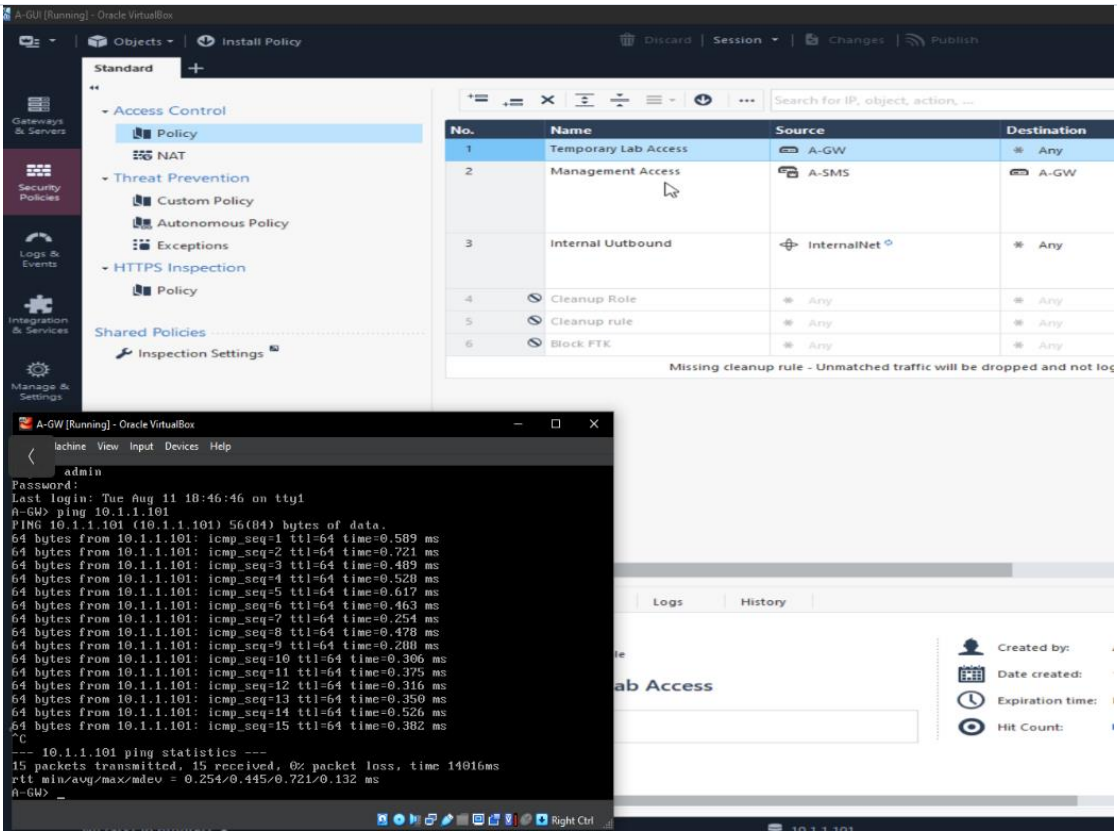

Figure 7: A-GW CLI — ping to A-SMS (10.1.1.101) succeeding with 0% packet loss.

From A-SMS, an initial extended ping to A-GW (10.1.1.1) — 601 packets sent over roughly ten minutes — recorded 100% packet loss. This is consistent with the Access Control policy not yet being installed on the gateway at that point in testing. A follow-up attempt to open an SSH session directly from the Gaia clish prompt (ssh admin@10.1.1.1) returned a command error (CLINFR0329); this is expected clish behaviour, since Gaia's restricted shell does not accept standard Linux SSH invocation syntax, rather than a sign of a connectivity fault. A subsequent ping test confirmed connectivity had been fully established, with all 4 packets returned successfully (0% loss, average 0.852 ms).

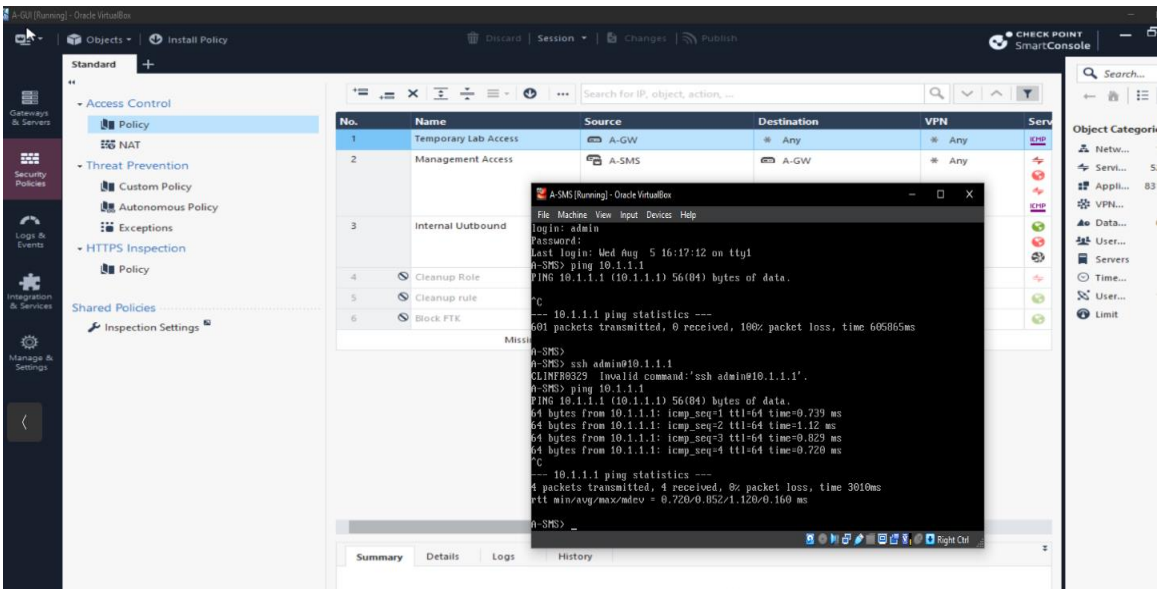

Figure 8: A-SMS CLI — initial ping to A-GW timing out, a clish SSH syntax error, then a successful re-test.

Taken together, Sections 3.1–3.4 satisfy the Task 1 key aspects: A-GW, A-SMS and A-GUI are installed and addressed correctly, the Security Management Server is licensed, and connectivity between the management workstation, SMS and gateway has been demonstrated and verified.

4. Firewall Rule Base & Traffic Control

4.1 Access Control Policy

The Access Control rule base was built directly in SmartConsole and captured from several angles during testing — with the Name and Source columns visible in Figures 7 and 8 (Section 3.4), and with the Services, Action and Track columns visible in Figure 9 below. Cross-referencing the two confirms they show the same three active rules, summarised in Table 3.

No.	Name	Source	Destination	Services	Action
1	Temporary Lab Access	A-GW	Any	ICMP echo-request	Accept
2	Management Access	A-SMS	A-GW	CPMI, HTTPS, SSH, ICMP echo-request	Accept
3	Internal Uutbound	InternalNet	Any	HTTP, HTTPS, DNS (domain-udp)	Accept
4–6	Cleanup Role / Cleanup rule / Block FTK	—	Any	SSH / HTTP / HTTP	Drop (disabled)

Table 3: Access Control rule base, consolidated from Figures 7–9. All Track values are Log.

Rule 2 (Management Access) permits the specific management-plane traffic the SMS needs to reach the gateway — CPMI for SIC/policy communication, HTTPS and SSH for administration, and ICMP for reachability testing — scoped tightly to A-SMS as the source rather than left open. Rule 3 (Internal Uutbound) permits general internal-to-outside web and DNS traffic. Rules 4–6 are prepared Drop rules (for SSH and HTTP) that were disabled during testing rather than enforced.

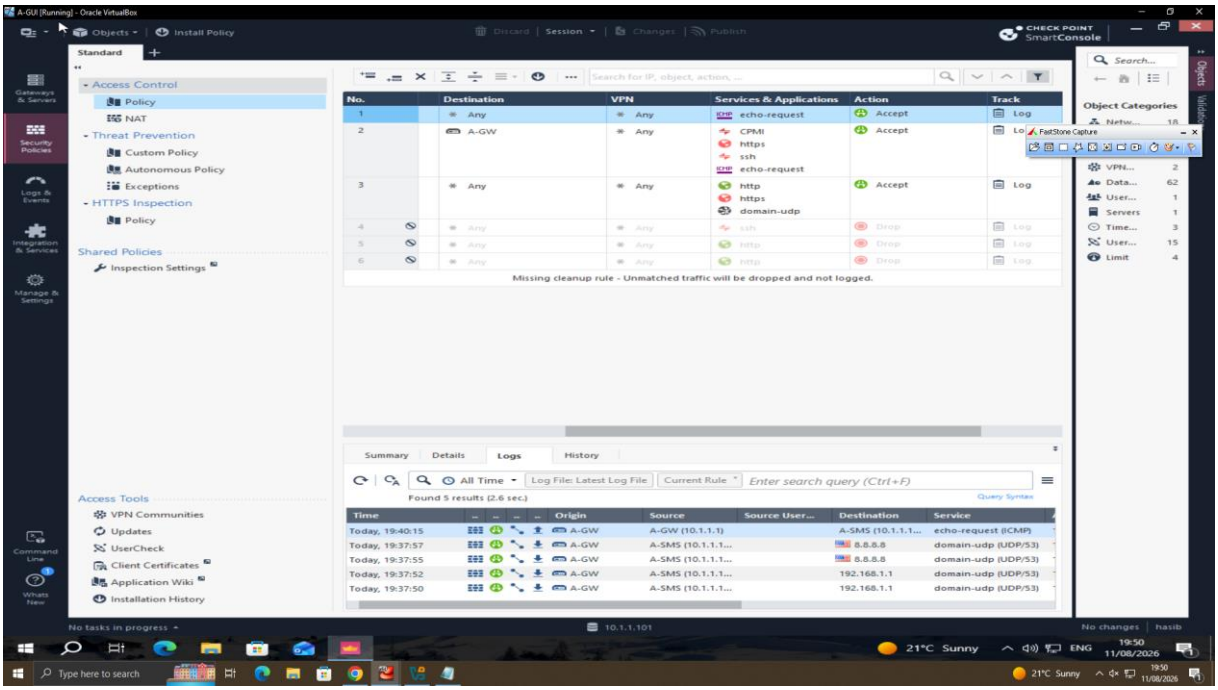

Figure 9: SmartConsole Access Control policy — full rule view including Services, Action and Track columns.

In all captures, SmartConsole flags “Missing cleanup rule — Unmatched traffic will be dropped and not logged.” Traffic that matches nothing above is still denied by the implicit default-drop behaviour of the gateway, but without an explicit, enabled cleanup rule that denial is not logged. Enabling and logging

an explicit cleanup rule as the final rule is recommended so that unmatched — and potentially unwanted — traffic is visible in Logs & Monitor rather than silently dropped.

4.2 Traffic Logging & Verification

Logging was verified through the Logs & Events view. The Favorites tab (Figure 10) confirms both Audit Logs and standard Logs views are available and populated.

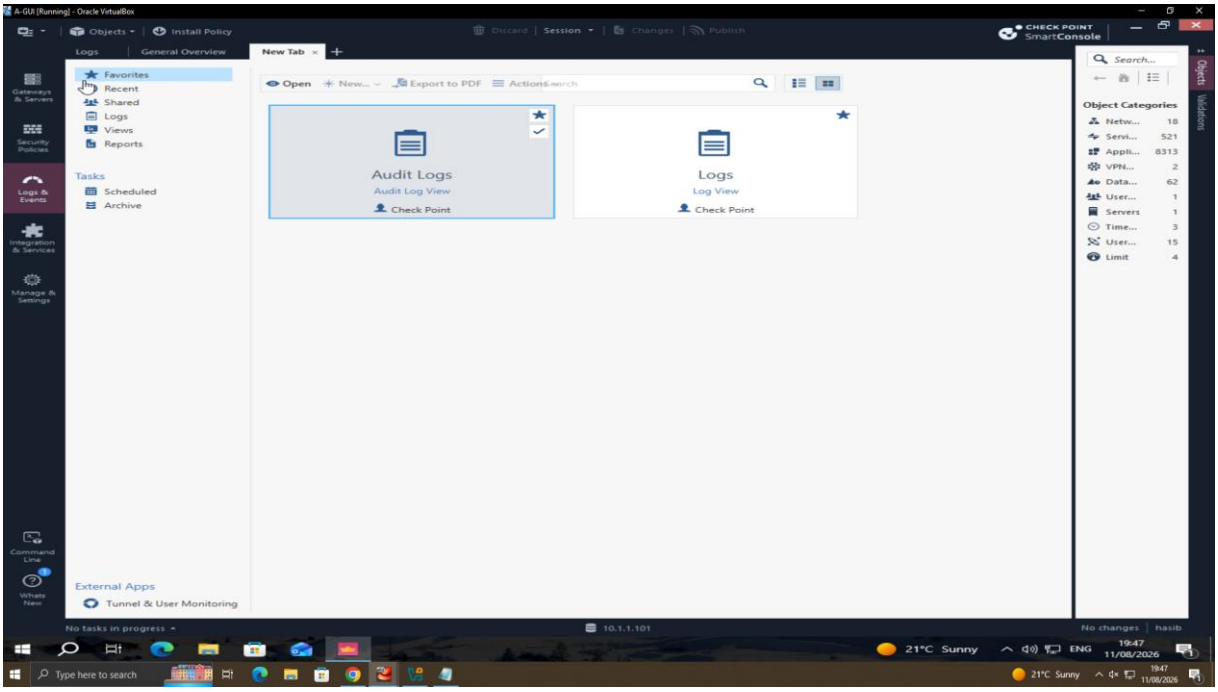

Figure 10: *SmartConsole Logs & Events — Favorites view, confirming Audit Logs and Logs are populated.*

A detailed query against the firewall log (fw.log) returned 27 results, including echo-request (ICMP) traffic between A-GW and A-SMS matched against the Management Access and Temporary Lab Access rules, and domain-udp (DNS) traffic from A-SMS to external resolvers (8.8.8.8) and an internal resolver (192.168.1.1), all matched against the Standard policy and recorded with a visible timestamp and originating gateway. This confirms that traffic is being evaluated against the intended rules and that the corresponding Track: Log setting is producing usable log entries.

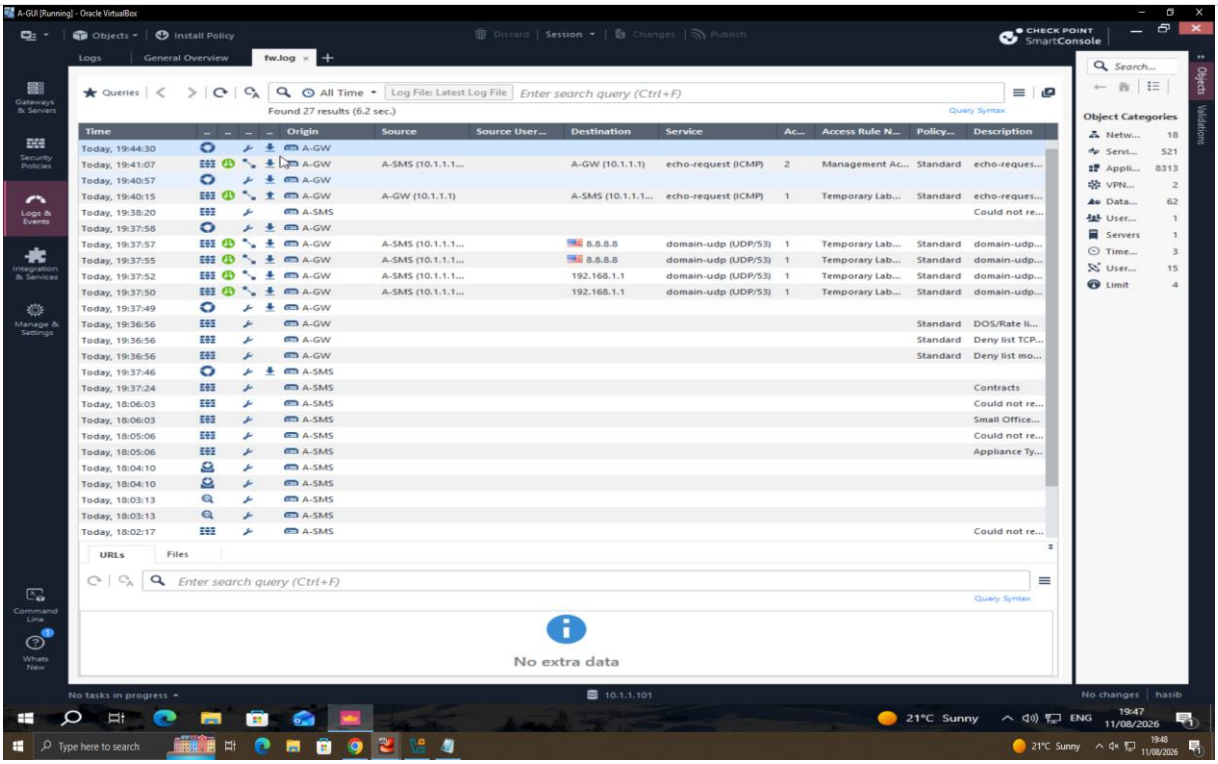

Figure 11: *fw.log detail — 27 logged events, including ICMP and DNS traffic matched against the Management Access and Temporary Lab Access rules.*

5. Conclusion

This stage of the enterprise network security implementation has successfully deployed and licensed a Check Point Security Management Server, connected it to SmartConsole, and verified end-to-end connectivity across the core management segment (A-GW, A-SMS, A-GUI). An Access Control rule base is in place and has been validated against live traffic logs, demonstrating that the gateway is enforcing — not merely displaying — the configured policy. Licence auditing via SmartUpdate also identified a concrete blocker for the Task 2 added-advantage items: the evaluation contracts covering IPS and Anti-Virus expired in November 2024, which explains why those blades are not yet active and sets a clear next step.

The added-advantage items under Task 2 (IPS, anti-malware, identity awareness) and the full scope of Task 3 remain outstanding, as summarised in Table 1 (Section 1.1) and detailed in Sections 4.3 and 5. Completing and evidencing these items is the primary remaining step before this report is ready for submission.

7. Attachment

1. Video link: Click Link
2. Presentation Link: Click Link