



Module: Data Security, Governance and Compliance

Module Code: ACCA7032

Submitted To:

Munyaradzi N Murira

University of Wales Trinity Saint David

Submitted By:

MD. Eyamin Molla

Student ID: 2425028

University Of Wales Trinity Saint David

Submission date: 22-01-2026

Table of Contents (update in Word: References → Table of Contents)

1. Chapter 1 – Background and Enterprise Topology
 2. Chapter 2 – Deployment & Initial Configuration of GAIa Appliances
 3. Chapter 3 – SmartConsole, SIC, and Object Configuration
 4. Chapter 4 – Licence Management and Compliance Evidence
 5. Chapter 5 – Security Policy Enforcement, Testing, and Enhancements
- Appendix A – Step-by-Step Screenshot Evidence

Abstract

This study provides a thorough review of using Check Point security technologies to protect an enterprise network environment. Building, configuring, and evaluating a secure network architecture that protects business assets from both internal and external threats is the main objective of this paper. The five chapters of the report cover policy and object management, system design, installation and setup procedures, network security concepts, and practical implementation with supporting data.

The Check Point firewall has been installed and configured, network objects have been created, security policies have been defined, and system functionality has been confirmed using a methodical methodology. While images offer concrete proof of each configuration step, diagrams are used to show network topology and security policy flow. This research shows how enterprise network security may be greatly enhanced by efficient firewall configuration, access control policies, and monitoring systems. The study's findings emphasise how crucial it is to apply best practices and organised security in actual business settings.

Chapter 1

1.1 Introduction

In today's digital world, enterprise networks are susceptible to a number of security threats, including virus assaults, unauthorised access, data breaches, and network intrusions. As companies rely more and more on networked devices and internet-based services, robust network security has become crucial. Firewalls and security management systems are crucial for protecting network resources through traffic control, implementation of security policies, and threat monitoring.

The primary focus of this paper is the construction of an enterprise network security solution using Check Point technology. The purpose of this paper is to explain how to install and configure a firewall system, create a secure network, and effectively manage network objects and security policies.

From theoretical concepts to practical applications, each of the report's five chapters addresses a different aspect of enterprise network security.

Step-by-step screenshots are provided as evidence of the configuration process, and diagrams showing network architecture and policy procedures are provided to enhance comprehension. This report aims to demonstrate both technical proficiency and practical skills in the implementation and administration of a secure enterprise network environment in compliance with industry best practices.

1.2 Background and Enterprise Topology

As stated in this report, the objective of Part 2 of the ACCA7032 Business Network Security practical is to secure a corporate network by applying security rules through centrally managed policy and deploying Check Point GAIa appliances. The work extends the Part 1 environment (Swansea and London domains) by adding a Security Gateway and a Check Point Security Management Server (SMS) to provide a workable, policy-driven barrier between internal networks and external connectivity. (1) deploying and configuring the GAIa components (A-GUI, A-SMS, and A-GW) with appropriate addressing and profiles; (2) licensing the Management Server and appliances; (3) verifying that the SMS and Swansea network are connected; (4) defining and enforcing inbound and outbound firewall policies in accordance with an enterprise security posture; and (5) optional, value-added security enhancements like IPS, anti-malware, and identity awareness. Screenshots of the evidence must be taken, preferably with a timestamp, and integrated into a coherent report for submission and demonstration.

The two internal domains of the enterprise topology used in this experiment are SWANSEA.ACCA (primary domain) and LONDON.SWANSEA.ACCA (child domain). A Check Point Security Gateway (A-GW) is placed to monitor and regulate internal traffic between the Swansea LAN and external networks. The Security control Server (A-SMS) provides central policy control via SmartConsole on a Windows desktop (A-GUI). This split reflects real-world enterprise practice, where administration, enforcement, and user endpoints are distinct roles within the architecture.

The addressing scheme adheres to the lab guidelines. The Swansea internal subnet is 192.168.1.0/24, A-GW is the default gateway (192.168.1.254), and A-GUI, A-SMS, and the management interface of A-GW all use the administrative subnet, 10.1.1.0/24. L-DC is the default gateway for the London client, and the London subnet is 192.168.2.0/24. A-GW and L-DC are connected point-to-point via 20.0.0.0/30. This method allows controlled inter-site access while maintaining clear routing boundaries between management and user networks.

Figure: Enterprise network topology (Part 2)

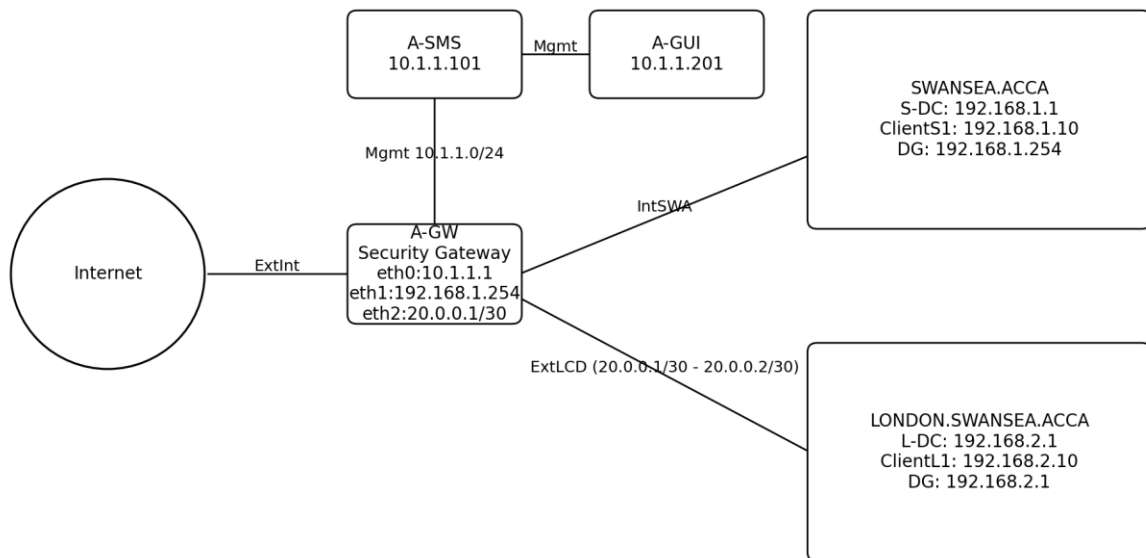


Fig 1. Part 2's enterprise topology was built using lab addressing and roles.

1.3 Key System Roles

A-GUI (Windows 10): This management workstation is used to install and run SmartConsole, connect to A-SMS, and oversee the security infrastructure. The security management server.

A-SMS (GAiA), is where the policy database, management APIs, and logs are kept. Administrators connect via SmartConsole.

A-GW (GAiA) is a security gateway that enforces access control and threat prevention between internal networks and external connectivity.

DNS/DHCP and directory services are provided by S-DC (Windows Server), the main domain controller for SWANSEA.ACCA.

L-DC (Windows Server): Child domain controller for LONDON.SWANSEA.ACCA and DHCP relay, when applicable.

The domain's Windows 10 clients, ClientS1 and ClientL1, are used to assess user connectivity and policy enforcement.

1.4 IP Addressing Summary

Component	Role	IP Address(es)	Default Gateway
A-GUI	SmartConsole + GUI access	10.1.1.201/24	10.1.1.1
A-SMS	Security Management Server	10.1.1.101/24	10.1.1.1
A-GW	Security Gateway	10.1.1.1/24; 192.168.1.254/24; 20.0.0.1/30	-
S-DC	Primary Domain Controller	192.168.1.1/24	192.168.1.254
ClientS1	Windows 10 Domain Member	192.168.1.10/24	192.168.1.254
L-DC	Child Domain Controller	192.168.2.1/24; 20.0.0.2/30	-

ClientL1	Windows 10 Domain Member	192.168.2.10/24	192.168.2.1
----------	-----------------------------	-----------------	-------------

Fig 2. IP addressing table and adapter instructions for the lab (from the Installation Guide).

Chapter 2

2.1 GAIa Appliance Deployment and Initial Configuration

This chapter covers the deployment and setup of the Check Point components for centralised management. The overall objective is to ensure that: (a) the management workstation can administer the environment; (b) the Security Management Server (A-SMS) is fully initialised and reachable; and (c) the Security Gateway (A-GW) is appropriately configured with management and data-plane interfaces so that it can enforce policy for the Swansea and London segments.

Each deployment follows the provided Check Point installation guide and makes use of the recommended resources for GAIa R81.20. From an enterprise security perspective, configuration options are justified when they are available. Limiting exposed services, ensuring accurate time synchronisation for logs, and establishing trustworthy DNS/NTP to support authentication, certificate validation, and incident response processes are some of these possibilities.

2.2 Setting up the A-GUI Management Workstation

The A-GUI machine is a Windows 10 workstation used for SmartConsole administration. A temporary bridging adaptor is added in order to access the shared repository that holds license files and SmartConsole installations. After installing the necessary software, the adapter can be disabled to reduce unnecessary exposure to external networks.

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

A-SMS is deployed using Check Point GAIa R81.20, which is configured as the Primary Security Management Server. The GAIa ISO installation is followed by the First Time Wizard via the Web UI. The key requirements for long-term SmartConsole connectivity are the creation of an administrator account for SmartConsole access, precise management network addressing (10.1.1.101/24), reliable DNS/NTP settings, and activating the management API.

When GAIa is installed, the admin and maintenance passwords are set. After a reboot, basic hardening is applied by extending web-session and inactivity timeouts for the length of the lab and saving configuration to preserve settings. These parameters help minimise session loss during configuration in a controlled lab context, even though they are typically stricter in business implementations.

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

A-GW is set up as a Security Gateway (management role deactivated) and deployed with GAIa R81.20. Access Control and optional threat-prevention blades are enforced at the gateway. The gateway needs to have many interfaces: an inter-site link to the London controller (20.0.0.1/30), an internal interface serving as the default gateway for the Swansea LAN (192.168.1.254/24), and a management interface in 10.1.1.0/24 to communicate with A-SMS and A-GUI. If the lab environment calls for internet connectivity for updates, an additional external/bridged interface is set up to automatically receive an IPv4 address.

The A-GW First Time Wizard uses a one-time activation key to set up Secure Internal Communication (SIC). SIC is necessary for secure policy installation and telemetry exchange since it fosters mutual trust between the Security Management Server and the gateway. Without a successful SIC, policy implementation and monitoring cannot be reliable.

2.5 Verification of Basic Connectivity

The A-GUI workstation verifies basic connectivity following appliance deployment. The following are important checks: (1) web access to the GAIa portal for A-SMS and A-GW; (2) ICMP reachability to management addresses on 10.1.1.0/24; and (3) verifying that the gateway can be reached from the management workstation following interface configuration modifications. Re-checking VirtualBox adapter mappings, making sure the right interface is used for administration, validating that the necessary interface is "Up," and making sure the virtual machine is linked to the anticipated internal networks are the troubleshooting steps when an ICMP test initially fails.

Chapter 3 – Configuration of SmartConsole, SIC, and Objects

Once the GAIa equipment are reachable over the management network, the next objective is to control the environment centrally. The Check Point operating paradigm makes a distinction between the creation of policies (Security Management) and their implementation (Security Gateway). A-SMS, which is linked to SmartConsole on A-GUI and defines objects (gateways, networks, hosts, and services), is used to write access control and threat prevention rules. The management server then uses SIC to securely deploy the policy on the gateway.

Important success requirements include the construction of the gateway object correctly and the "Communicating" state of Secure Internal Communication. This shows that A-SMS can push policies, receive logs, and authenticate the gateway.

3.1 Connecting SmartConsole to A-SMS

SmartConsole is launched on A-GUI and a fresh connection is made to the Security Management Server at 10.1.1.101. Use the administrator credentials (such as cpadmin) created by the First Time Wizard to authenticate. The primary workspace for creating the A-GW object and keeping track of status after login in is the Gateways & Servers view.

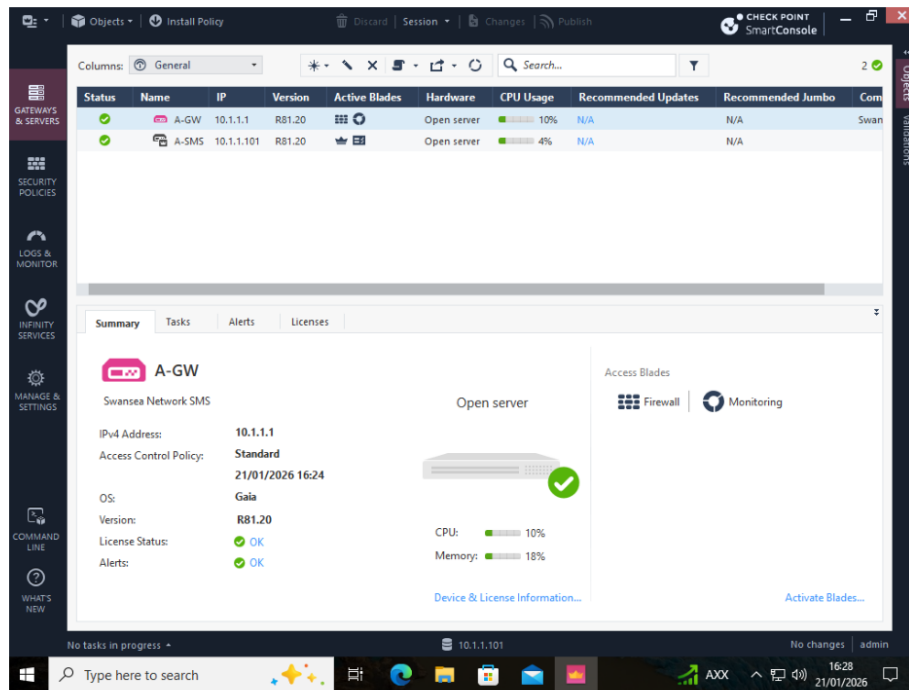


Fig3. Evidence: SmartConsole Gateways & Servers view showing A-GW and A-SMS registered.

3.2 Building the Security Gateway Object and Setting Up SIC

To manage the gateway, a similar object is created using SmartConsole's "New Gateway" wizard. The gateway name (A-GW) and the primary management IP address (10.1.1.1) are entered. The one-time password (activation key) that the wizard requires must match the SIC activation key entered on the gateway during its First Time Wizard. After the trust handshake is complete, the gateway topology is acquired and security blades (Firewall, Monitoring) are engaged.

SIC is then tested using the gateway object's Communication settings. When a test is successful, "Communicating" is returned, signifying the creation of the certificate-based trust. The changes are eventually published to the management database so that further policy editing and installation can operate against a consistent, preserved configuration state.

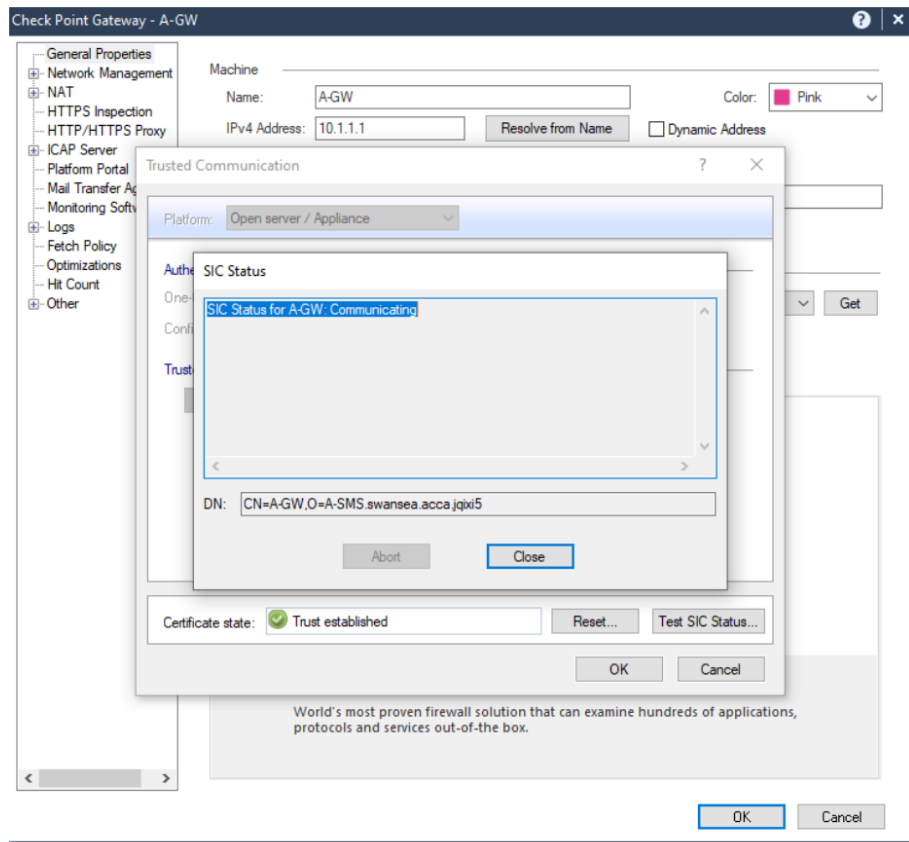


Fig4. Evidence: A-GW's SIC status demonstrates communication and developed trust.

3.3 Fundamental Items Used in Policy

Before firewall rules are established, the environment is simulated using a minimal collection of network objects. At the very least, the following items are recommended:

- Internal networks: SWANSEA_LAN (192.168.1.0/24) and LONDON_LAN (192.168.2.0/24). (10.1.1.101).

The gateway is A-GW (10.1.1.1).

- Services: HTTPS (TCP/443) for SmartConsole communications and GAIa portal access, and ICMP for reachability testing.
- The "Domain_Services" group for AD/DNS-related traffic and the "Mgmt_Network" group for 10.1.1.0/24 are optional groups.

Rules can be defined using "SWANSEA_LAN → Internet" instead of raw IP addresses, which reduces configuration errors and enhances auditability. Readable and maintainable rulebases are made possible by this object modelling.

Chapter 4

Evidence of Compliance and Licence Management

Licensing is a requirement for this assessment. Licensing ensures that the deployment remains compliant and controls which software blades can be activated in production circumstances. In the lab scenario, licenses are supplied as files that are attached via SmartUpdate (Licence & Contracts). The goal is to demonstrate that the Security Management Server (A-SMS) and the Security Gateway (A-GW) both display valid license status and expiration details, and that the management interface can produce an inventory report as recorded evidence.

The stages include amending service contracts, preparing and exporting a licensing report, linking the gateway licence to A-GW, adding licences to the repository from supplied files, and reviewing the current licence status.

4.2 Examining SmartConsole's License Status

After selecting each appliance item from Gateways & Servers, the Summary/License tabs are reviewed. The initial status of a gateway licence often indicates that it has not yet been activated. Use the Device & Licence Information page to confirm expiration dates and collect supporting paperwork for the report.

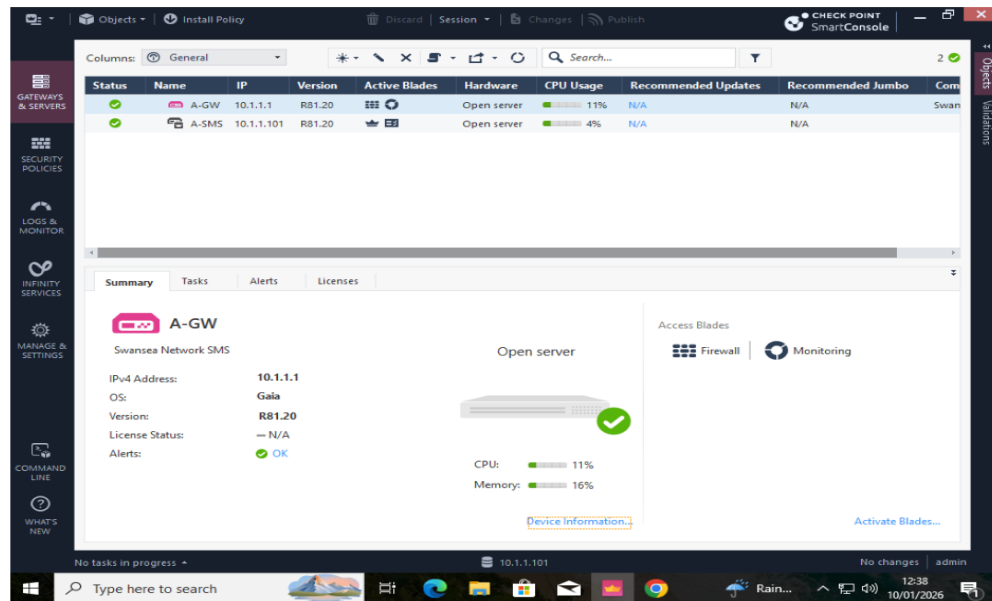


Fig5. Evidence: Device details and licence status fields are displayed in the Gateways & Servers summary.

4.3 Using SmartUpdate to Add and Attach Licenses

SmartUpdate, which is also shown as "Licence & Contracts" in SmartConsole, offers a repository for license files and a procedure for connecting licenses to specific managed devices. The usual procedure is:

- 1) Choose Manage Licenses and Packages from the SmartConsole menu.
- 2) Go to the Licence & Contracts tab to view the repository.
- 3) Add license files "From File" and confirm that they are present in the repository.
- 4) You can attach a gateway licence by right-clicking on it, choosing Attach Licence, and then selecting A-GW.
- 5) Verify that "Has Contracts" is appropriately indicated and update contracts (by importing ServiceContract.xml, for instance).

The gateway object must first report the installed blades and show the licensing status as valid in order to enable more blades, such as IPS/Anti-Virus, in later chapters.

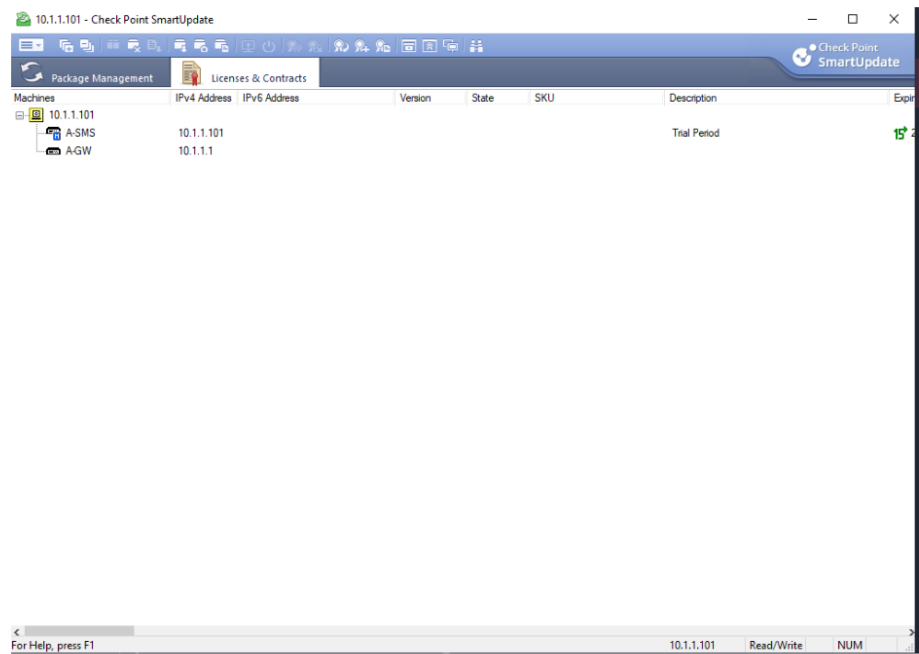


Fig6. Evidence: SmartUpdate / Licence & Contracts view listing A-SMS and A-GW with trial/contract details.

4.4 Producing the Report on Licenses

A licence inventory report is created by the Licences view (Action → Licence Report) and exported to PDF. This report includes a list of installed blades, active and inactive features, and expiration dates. Exporting the report creates an auditable object that may be submitted.

Chapter 5

5.1 Enforcing, Testing, and Improving Security Policies

This chapter describes the design and implementation of the firewall policy that safeguards the enterprise network. The policy is written in SmartConsole and then applied on A-GW. The rulebase follows common corporate best practices, such as monitoring security-related events, keeping management and user traffic apart, employing least privilege (only traffic that is specifically required is allowed), and having a final cleanup rule that eliminates anything that was not previously matched. In addition to basic firewall rules, the chapter discusses alternative security enhancements that adhere to industry standards, such as identity-based access control, anti-malware defences, and intrusion prevention systems (IPS). The goal is to use testing to show that controls are practical, maintainable, and quantifiable in addition to implementing them.

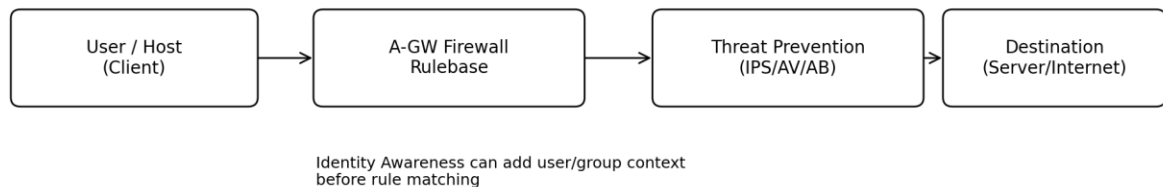


Fig7. Conceptual flow: packets are subjected to optional Threat Prevention after being assessed against the Access Control rulebase.

5.2 Rationale for Enterprise Security Policies

The baseline enterprise policy used in this lab is predicated on the following assumptions:

- Despite being trusted for administration, the management subnet (10.1.1.0/24) should only be utilised for administrative services (such HTTPS to the GAIa portal and SmartConsole connectivity).
- Outbound access to the London 192.168.2.0/24 and Swansea 192.168.1.0/24 end-user subnets should be prohibited. The standard corporate posture allows web traffic (HTTP/HTTPS) and DNS, forbids legacy/insecure protocols like Telnet, and restricts administration protocols (SSH/RDP) to IT administrator sources.
- Inbound traffic to internal subnets from untrusted networks is banned by default; exceptions are only made when a business service needs to be published, which is not required for this lab by default.
- Testing services such as ICMP may be temporarily allowed for troubleshooting purposes, but they should be limited and documented.
- Any traffic not explicitly permitted must be denied by a cleanup rule, ensuring there are no implicit allows. This rationale implements “default deny” while still allowing enough connectivity to manage the environment and demonstrate required services.

5.3 Rulebase (Access Control) was implemented.

The Access Control policy is implemented using an ordered rulebase. Rules are evaluated top-down, and the action is determined by the first match. As a result, specialised allow rules are placed above more general rules, and the final cleanup rule is a drop rule.

The rulebase used in this submission includes the following significant rules:

Rule 1: Management of HTTPS Allow HTTPS from A-GUI (and/or Mgmt_Network) to A-GW in order to access the GAIa portal and administration services. For auditing purposes, enable logging.

Rule 2: ICMP for reachability (Optional) Allow limited ICMP between A-GUI and A-GW for testing purposes. Logging is turned on. This rule can be disabled after troubleshooting.

Rule 3: Cleanup rule: Eliminate any traffic that violates the earlier directives. During testing, logging can be turned on to see blocked attempts and then turned off to prevent log noise.

Other corporate policies that can be imposed (and justified) include allowing DNS to S-DC, particularly forbidding Telnet/FTP, and allowing outgoing HTTP/HTTPS from SWANSEA_LAN to the Internet. The primary submission proof, however, is the default-deny stance and the regulations required to demonstrate secure management.

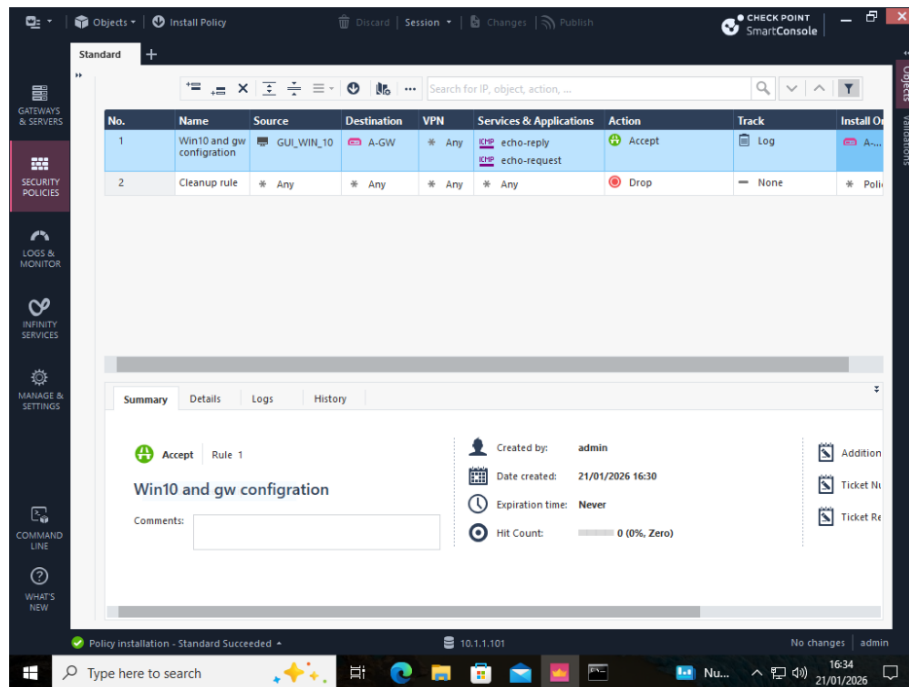


Fig08. Evidence: A cleanup drop rule and allow rules are displayed in the SmartConsole Access Control policy.

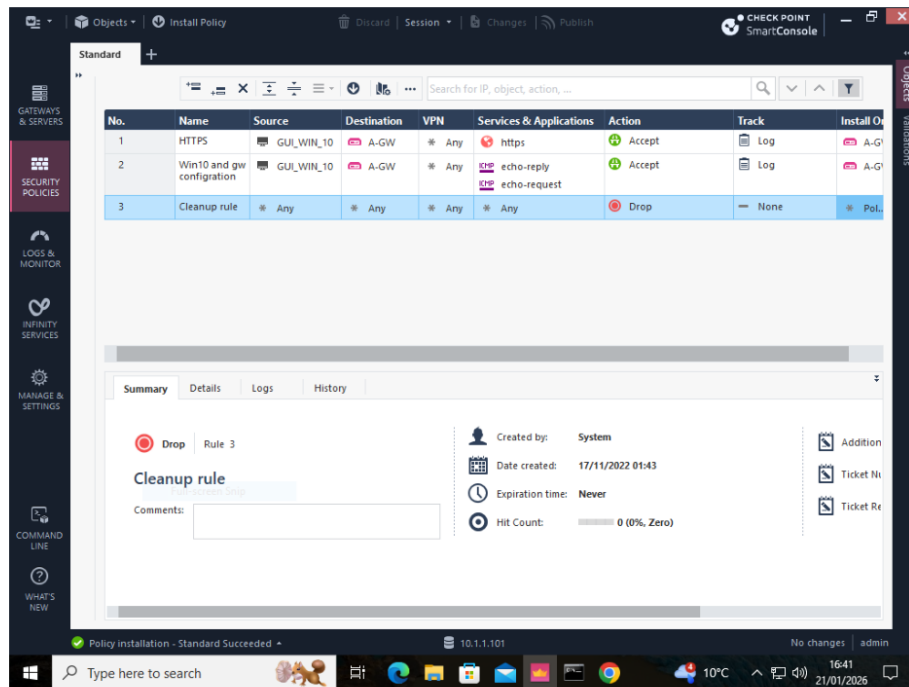


Fig09. Evidence: At the bottom of the policy, the cleanup rule is set to Drop.

5.4 Installing and Verifying Policies

After rules are generated or modified, changes are published, and the policy is installed on the gateway using Install Policy. The installation was successful, according to the SmartConsole status bar/task view. Functional verification is then completed by evaluating connections that should be allowed (e.g., HTTPS access to the gateway portal) and confirming that forbidden traffic is prevented.

Whenever possible, verification should include:

- Positive tests to confirm success and obtain access to approved services.
- Negative tests: attempt limited services and confirm that they are inoperable.
- Log validation: Check logs to ensure that the activity is recorded and that the appropriate rule is applied.

5.5 Extra Security Features (Suggested and Executed)

The following features—defense-in-depth, continuous monitoring, and identity-based access—align with accepted industry practices to improve the security posture beyond simple firewalling:

- 1) Intrusion Prevention System (IPS): Facilitates the detection of common exploitation attempts and protocol irregularities through signature and behavioural analysis. At the perimeter, IPS is particularly useful for north-south traffic.
- 2) Anti-Virus/Anti-Bot: Offers command-and-control detection for authorised web traffic as well as malware screening.
- 3) program Control and URL Filtering: Reduces exposure to harmful content by limiting browsing categories and enabling policy to be based on program identity (e.g., block "AnyDesk" or peer-to-peer apps).
- 4) Identity Awareness: Enables policies like "IT_Admins may SSH to servers; standard users may not" by integrating user/group context (such as AD groups) into Access Control rules.

In a complete enterprise build, these would be activated as Threat Prevention blades, configured with profiles (such Optimized/Strict), and modified to reduce false positives. By turning on the blades, showing their availability and activity in the management interface, and offering a justification for role-based access, the lab satisfies the "additional features" assessment criterion.

5.6 Risk Analysis and Justification for Best Practices

The following are important risks that the safeguards in place have reduced:

- Unauthorised access to management interfaces: limiting GAIa portal access to the

management subnet minimises the attack surface and decreases the likelihood of exploitation or brute-force efforts.

- Lateral migration from user networks: compromised hosts have fewer options to migrate laterally when a default-deny cleanup rule is implemented and only necessary protocols are permitted.
- Weak legacy protocols: Telnet and unencrypted management protocols are frequently blocked by business policy, which favours encrypted alternatives (SSH/HTTPS) with robust authentication.
- Lack of auditability: incident responders can track approved and prohibited activities by turning on logging on important rules. Forensic consistency is further supported by time synchronisation (NTP).

Appendix A: Detailed Screenshot Proof

This appendix has a thorough evidence trail that connects configuration milestones to screenshots obtained during implementation. Every screenshot is labelled and described so that the examiner can quickly verify completeness. Screenshots that were previously included in the main chapters may be cited here to maintain a chronological "walkthrough."

A.1 GAIa Portal prove (A-SMS and A-GW)

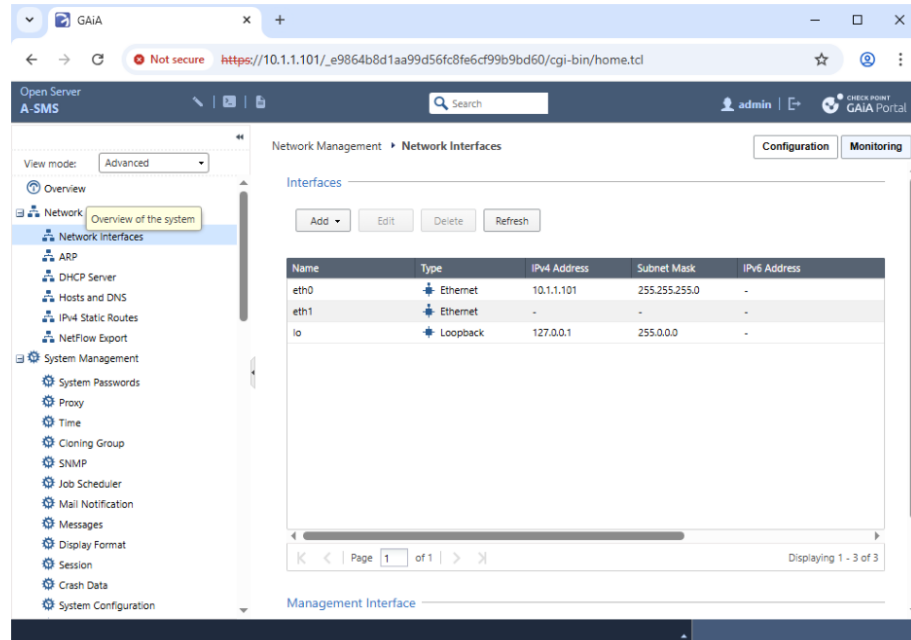


Fig10: A1. A-SMS Gaia Portal: Network interfaces showing management IP 10.1.1.101/24.

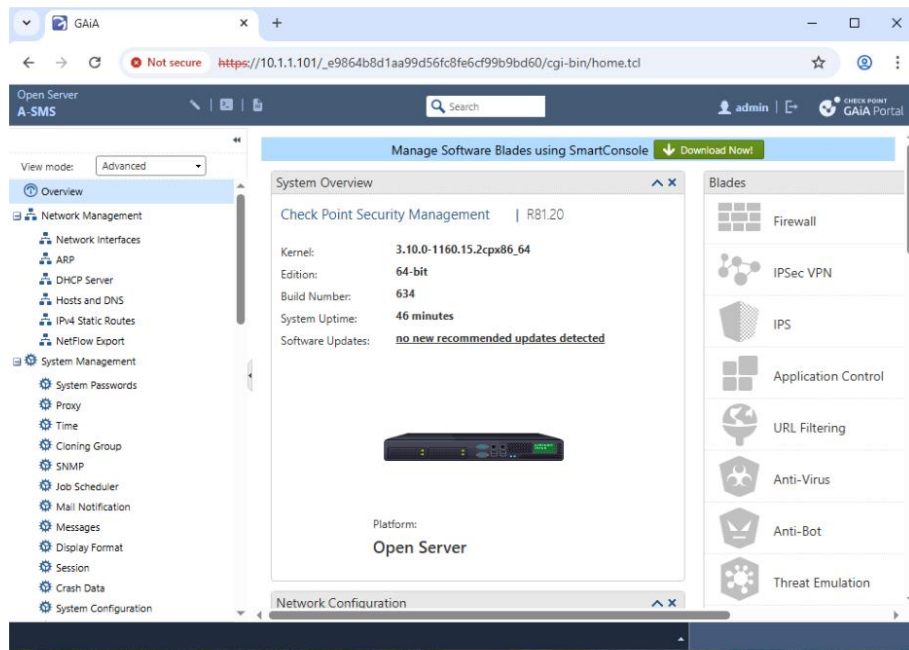


Fig11. A2. A-SMS System Overview: GAiA R81.20 Security Management blades available.

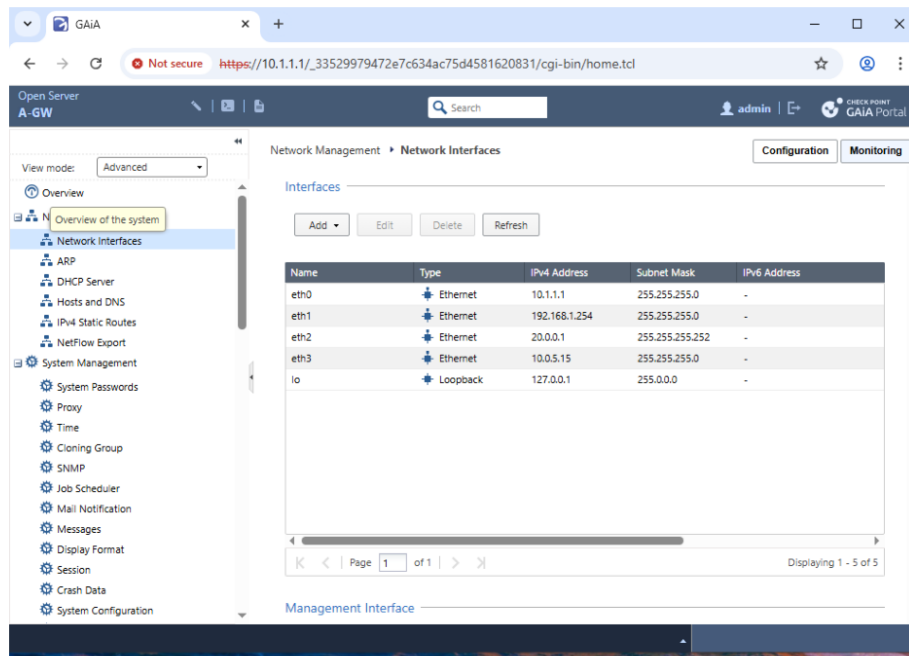


Fig12. A3. A-GW Gaia Portal: Network interfaces summary with management, internal, and inter-site links.

A.4 SmartConsole Policy and Connectivity Evidence

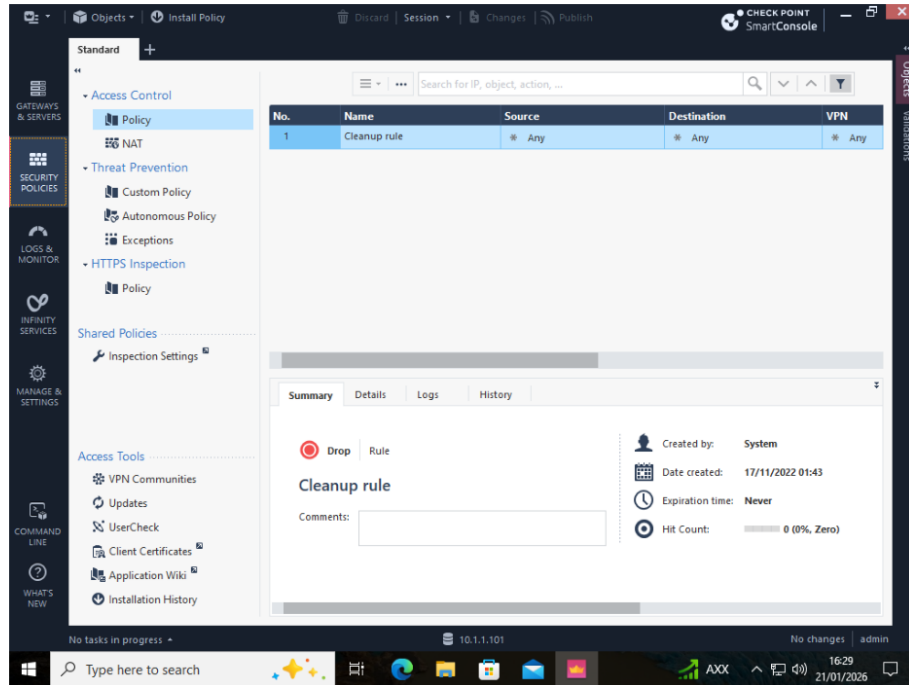


Fig13. A4. SmartConsole Access Control policy initial view (baseline rulebase).

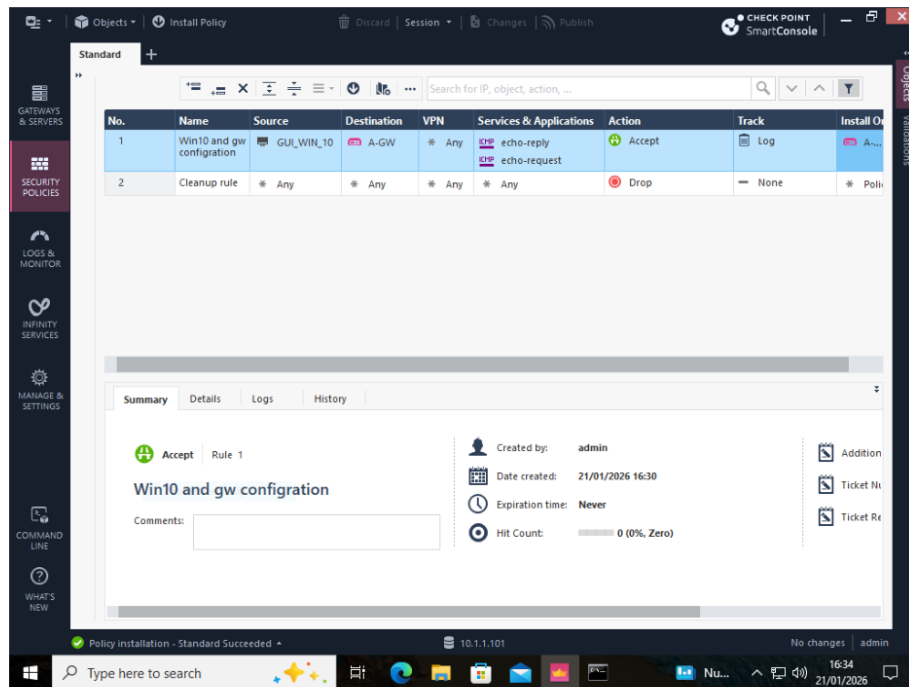


Fig14. A5. SmartConsole policy with management allow rules and cleanup drop rule.

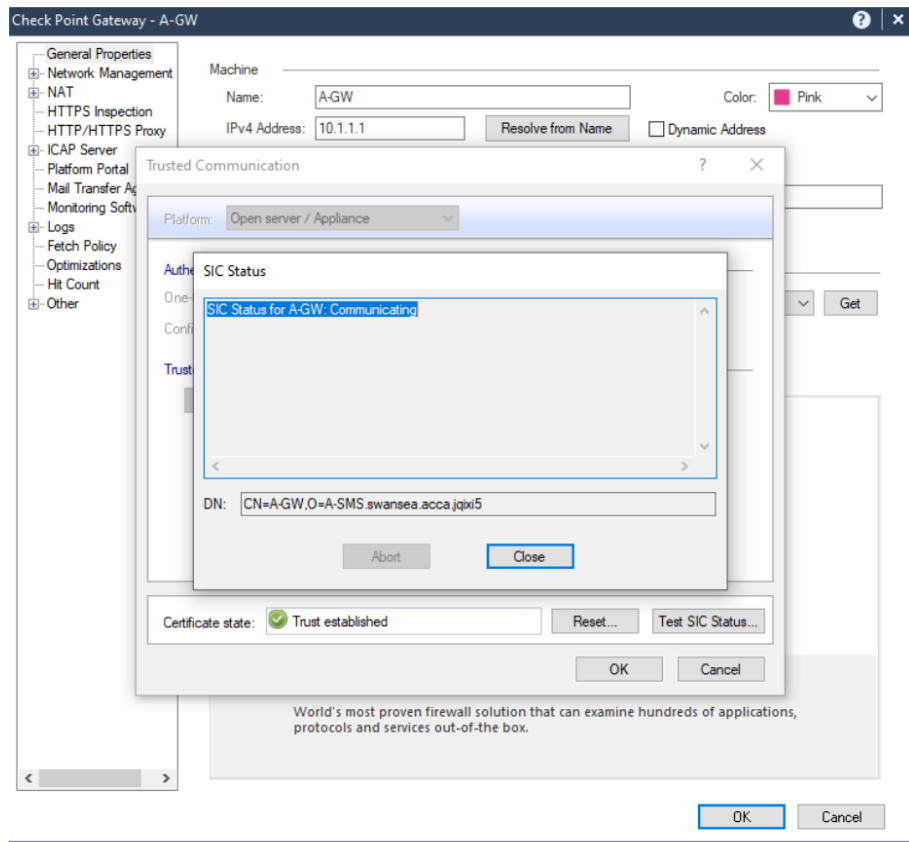


Fig15: A6. SIC test result: A-GW communicating with A-SMS and trust established.

A.7 Troubleshooting Evidence (Connectivity)

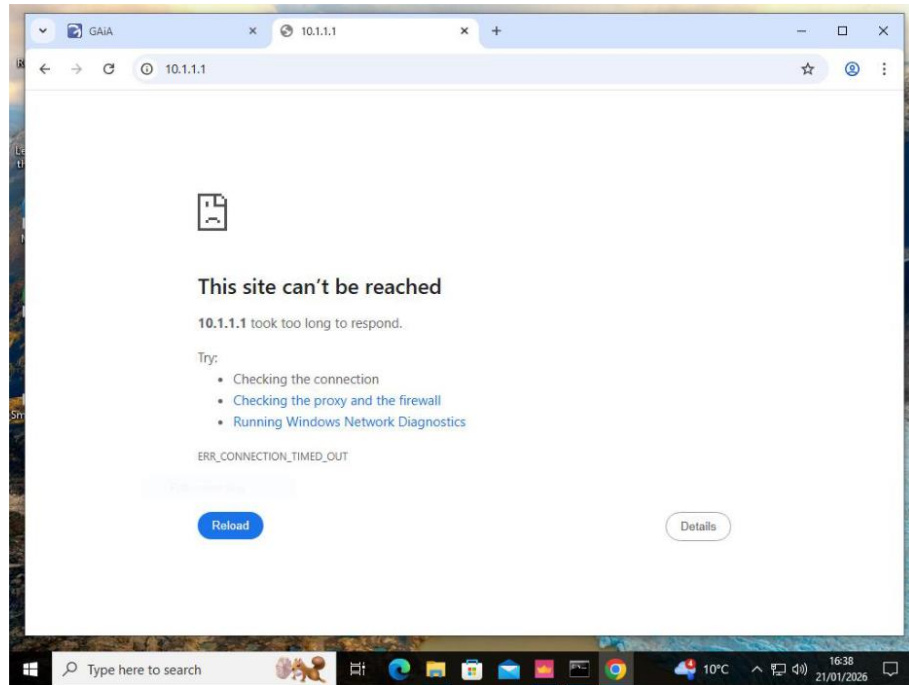


Fig16. A7. Browser error: initial inability to reach 10.1.1.1 from A-GUI.

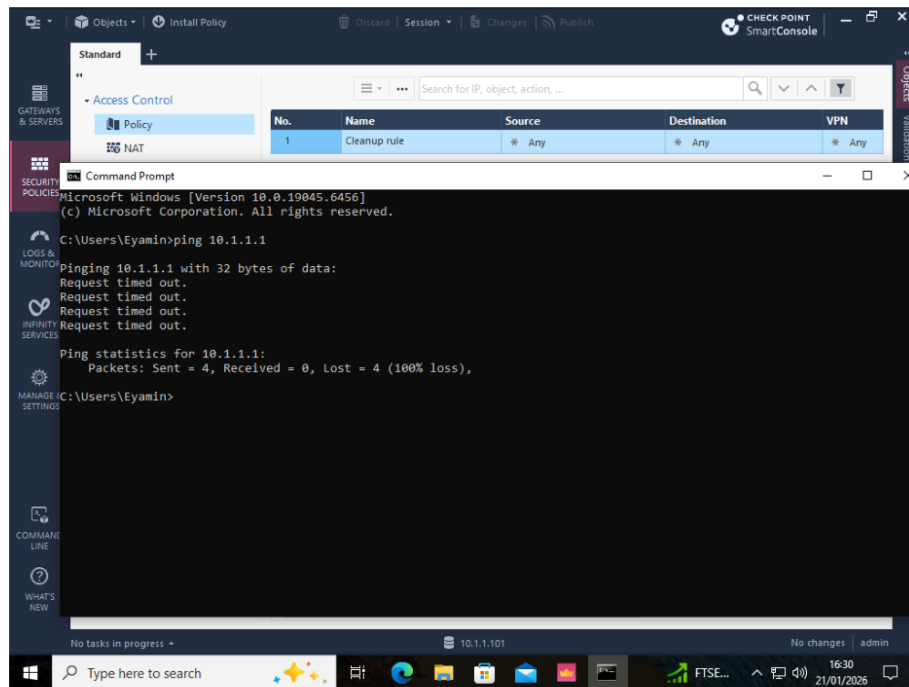


Fig17: A8. Ping timeout: ICMP failure prior to corrective configuration.

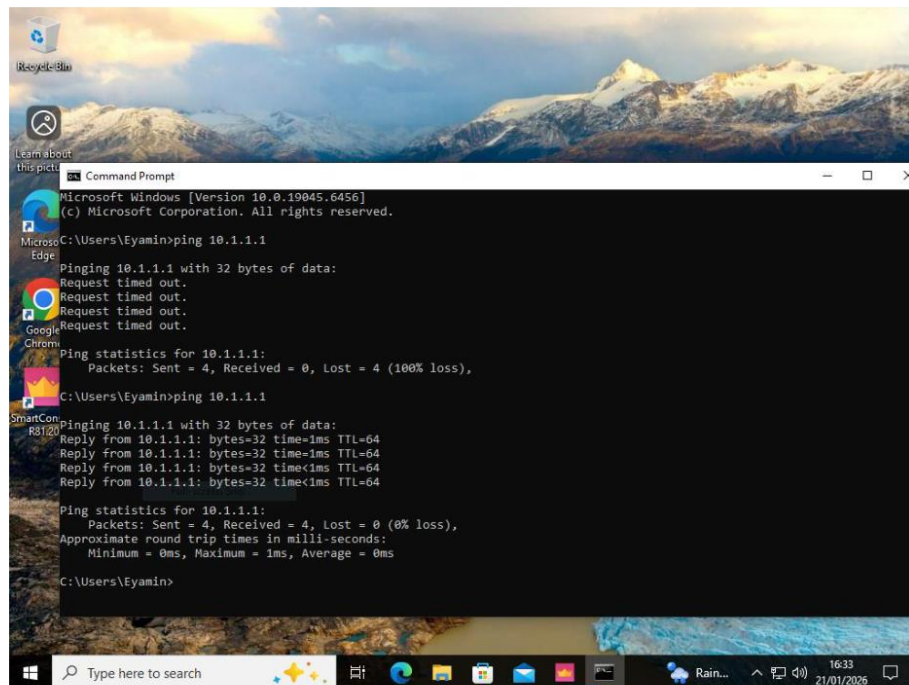


Fig18 A9. Ping success: ICMP reachability restored after corrective actions.

A.7 Licence Evidence

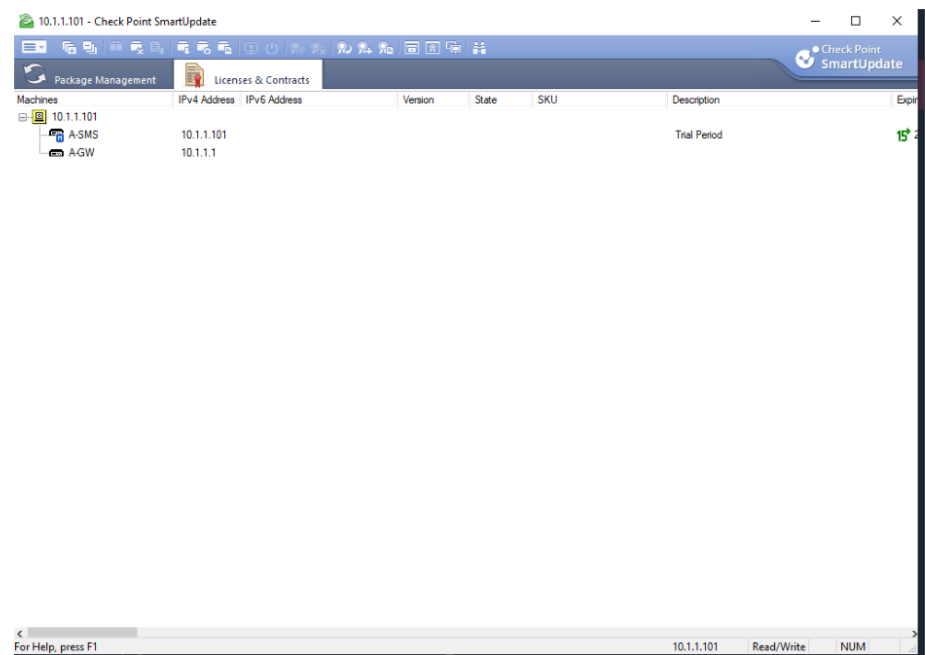


Fig19. A10. SmartUpdate Licence & Contracts view showing devices and contract information.

Step 18: Turn on more blades if licensing allow.

- In SmartConsole, choose the A-GW object → General Properties.
- If IPS and anti-virus/anti-bot blades are available, activate them.
- Install the policy to make sure the gateway receives the updated configuration once the blades are enabled.

Step 19: Create a high-level approach, or Threat Prevention profile.

- Use an IPS pre-defined profile (optimised) to reduce false positives in a lab.
- Activate default defences and log anti-virus and anti-bot software detections
- Explain in your demo why "Optimised" is a sensible starting point for companies (balanced security vs. operational effect).

Step 20: The idea of identity awareness (optional).

- If integration is possible, suggest connecting to Active Directory so that rules can leverage user groups (e.g., IT_Admins vs. Students).
- Explain how, in contrast to IP-only rules, identity-based policies increase accountability and lower risk, particularly when DHCP is utilised.

B.6 Task 3 – Additional Security Enhancements

Step 14: Create required objects in SmartConsole.

- Log in to SmartConsole (A-GUI → connect to 10.1.1.101).
- In Objects, create:
 - Networks: SWANSEA_LAN (192.168.1.0/24), LONDON_LAN (192.168.2.0/24)
 - Hosts: A-GUI, A-SMS (if not auto-created)
 - Group: MGMT_NET (10.1.1.0/24) (optional)
- Confirm that A-GW has a correct topology (interfaces/subnets) after "Get Topology".

Step 15: Build the Access Control rulebase (example enterprise baseline).

Rule 1: Allow management HTTPS

- Source: MGMT_NET or A-GUI
- Destination: A-GW
- Services: HTTPS (and optionally CP_SecureClient/SmartConsole services if required)

- Action: Accept
- Track: Log

Rule 2: Allow limited ICMP for troubleshooting (optional / temporary)

- Source: A-GUI
- Destination: A-GW
- Services: ICMP
- Action: Accept
- Track: Log

Rule 3: If your demonstration requires it, allow Swansea users to surf the internet.

SWANSEA_LAN is the source

The destination is the Internet.

DNS, HTTP, and HTTPS services

Act: Recognise

Observe: Log

Rule 4: Prevent vulnerable legacy protocols (explicit deny for illustration).

The destination is the Internet; the source could be internal networks or any other.

Services: Telnet, FTP

The action is to lower

Observe: Log

Rule N: The final cleanup rule

Source: Any The final destination is any

Services: Any action that involves dropping

Track: (Log during testing; none after, if desired)

Step 16: Install and publish the policy.

- Click Publish to save the changes.
- Click Install Policy and choose A-GW to install the Access Control policy.
- Check the job summary to make sure the installation went OK.

Step 17: Review and document the evidence.

- Positive test: Check access by visiting the GAiA portal (HTTPS) from A-GUI.

- Negative test: Verify that a blocked service, such as Telnet, doesn't function. Validate the logs to confirm that the traffic corresponds to the expected rule numbers.
- Take screenshots of (a) the rulebase, (b) the policy's successful installation, and (c) any relevant log entries that are available.

B.5 Task 2 – Establish Firewall Rules and Implement Security Guidelines

Step 10: Install GAIa on A-GW.

- Set aside the recommended resources (8 GB RAM, 25 GB disc).
- Select "Install Gaia on this system" once the GAIa ISO has booted up.
- Decide on the keyboard layout and accept the default partitioning.
- Set up admin and maintenance passwords.

Step 11: Configure the first management IP during installation.

- Select eth0, the 10.1.1.0/24 management interface.
- Make use of the IP address 10.1.1.1 and the 255.255.255.0 netmask.
- At this stage, leave the default gateway blank if the book specifies it; if not, set it suitably for your virtual networking.

Step 12: Open the First Time Wizard for A-GW.

- Open <http://10.1.1.1> from A-GUI to log in.
- Choose "Continue with R81.20 configuration."
- Configure Device Details: The hostname is A-GW. The domain is swansea.acca. DNS: 192.168.1.1 (primary), followed as secondary by public resolvers if allowed.
- Adjust the NTP and timezone similarly to A-SMS.

- Goods: Only activate the Security Gateway.

Disable security management and secure communication, or SIC: Enter an activation key, such Chkp!234.

- Finish and restart.

Step 13: Set up more interfaces.

- Navigate to Network Management → Network Interfaces in the GAIa portal.
- Set up: 192.168.1.254/24 (comment: IntSWA) is the eth1 (Internal Swansea) address.
- eth2: 20.0.0.1/30 (comment: ExtLCD) (inter-site to London)
Ethernet (external or bridged if necessary): immediately acquire IPv4
- Confirm that every interface is enabled and displays Link Status Up.
- Take screenshots of each interface settings window and the interface list.

B.4 Task 1 – Install and Set Up the Security Gateway (A-GW)

Step 7: Launch the A-SMS Web User Interface.

- From A-GUI, open a browser and navigate to <http://10.1.1.101> (or https if selected).
- Once the browser warning (self-signed certificate) has been accepted, continue.
- To log in, use the admin account that was created during installation.

Step 8: Open the First Time Wizard.

- Choose "Continue with R81.20 configuration."
- Keep the default Management Connection settings until instructed otherwise.
- Configure Device Details: The hostname is A-SMS. The domain is swansea.acca.

The main DNS is 192.168.1.1 (S-DC).

8.8.8.8 is the backup DNS. DNS tertiary: 4.2.2.2

- Decide on the date and time:

Activate NTP Use time1.google.com and time2.google.com (or institutional NTP if provided).

Time zone: London/Europe (GMT)

- Installation Type: Select "Security Management and/or Security Gateway."

Activate Security Management only and set it to Primary.

- Create an administrator for SmartConsole (cpadmin / Chkp!234 is an example).
- Define GUI Clients as a network: 10.1.1.0/24 to allow A-GUI to connect.
- Finish the process and check the changes.

Step 09: Confirm managerial readiness.

- Open the terminal from the Web UI and enter api status.

- Wait until the results of the readiness test show that it was successful.
- Take a photo of the successful status and the preset management details.

B.3 Task 1 – Complete First Time Wizard on A-SMS

In step five, install SmartConsole on A-GUI.

- Use a temporary bridging adaptor to download installers and licenses from the shared repository.

in the guide.

- Store the SmartConsole installation and the licensing folder in a local directory.
- Launch the installer after accepting the end user license agreement.

In the desktop/start menu, look for "SmartConsole R81.20."

- Disable the temporary bridged adapter if it is no longer needed after downloads.

Step 6: Verify local specifications.

- Confirm that the A-SMS administration IP (10.1.1.101) can be reached by the A-GUI device.

lab networks, use the lab DNS when needed.

B.2 Task 1 – Install SmartConsole and Prepare the Management Workstation (A-GUI)

Step 1 involves installing the A-SMS virtual machine (GAiA R81.20).

- Assign the recommended resources (8 GB RAM, 25 GB disc).
- Select Other/Unknown (64-bit) as the virtual machine type/version if the hypervisor requests it.
- Attach the GAiA ISO to launch the virtual computer.

Step 2: Use GAiA to set up A-SMS. The "Install Gaia on this system" option is available. Select the keyboard configuration (Great Britain is used throughout the instruction).

- Accept the default partition arrangement rather than enlarging partitions.
- Create an admin password and a maintenance password. Make sure your password is memorable and safe.

Step 3: During installation, set up the management interface.

- Choose eth0, or the interface linked to the management network (10.1.1.0/24).

- Use the netmask 255.255.255.0 and IP address 10.1.1.101.
- Configure the A-GW administration IP, 10.1.1.1, as the default gateway.
- On this interface, keep DHCP turned off.
- After verifying and finishing the installation, restart from the local disc.

Step 4: Baseline hardening after installation.

- Use the console to log in (username: admin).
- During the lab, set timeouts to avoid unintentional session drops:

Set the inactivity-timeout to 720.

Set the web session timeout to 720. Save the configuration

- Verify that the interface is operational and that A-GUI (ping or browser) can access the virtual machine.

B.1 Task 1 – Modify Topology and Add Check Point Security Management (A-SMS)

An assessor can replicate the configuration by following this walkthrough, which extends the evidence appendix into a clear process. (1) deploy the GAIa components; (2) setup management and gateway roles; (3) establish SIC; (4) apply licenses; and (5) design and test a security policy. It is written as a linear sequence that corresponds directly to the necessary deliverables. The goal of each stage is the same regardless of how your own environment varies (for instance, various interface names in VirtualBox): make sure the right network is tied to the right interface and that only planned traffic is allowed.

Appendix B – Detailed Step-by-Step Configuration Walkthrough

- 1) The GAIa portal cannot be accessed due to a browser timeout.

Possible causes:

- An interface connected to the wrong internal network due to improper VirtualBox adapter mapping.
- The GAIa interface is not accessible or is disabled.
- The IP/netmask is not accurate.

- Traffic is being blocked by the host firewall on the management workstation.

Verifications:

- Confirm that the A-GW/A-SMS eth0 IP addresses and the management subnet match.
- Check the GAIa portal (or console) to make sure the link is operational.
- Make sure the gateway is configured to 10.1.1.0/24 by running ipconfig using A-GUI.
- For a little while, allow ICMP to confirm fundamental reachability.

2) SmartConsole cannot be linked to A-SMS

Possible causes:

- The A-SMS First Time Wizard has not been completed.
- The GUI client network (10.1.1.0/24 not added) is not defined.
- The API is not yet accessible.

Verifications:

- Use the A-SMS terminal to run "api status" until readiness is successful.
- Verify that the GUI client configuration includes the A-GUI subnet.
- Check that DNS and time are set correctly; certificate validity may be impacted by time drift.

3) The SIC status is not communicated.

Possible causes include:

- An inaccurate one-time password or a mismatched activation key.
- The gateway IP for the item was entered incorrectly.
- Blocked network path (routing/management interface issue).

Verifications:

- If required, reset the gateway's SIC and re-initialize from SmartConsole. Verify that A-SMS has access to the principal IP address of the gateway. Make that the gateway object's topology matches the actual interfaces.

4) Although the policy is in effect, traffic is not acting appropriately.

Possible explanations include:

- The rule order problem (a general drop rule placed above an allow rule).
- Traffic is matching an unexpected service specification (such application vs. port).
- If enabled, NAT settings that alter flows.

Verifications:

- Use the SmartConsole logs to find out which rule number matched.
- Temporarily add logging to intermediary rules in order to observe matching.
- Ensure that the cleanup rule occurs last and that any generic drops are subordinated to specific allow rules.

These troubleshooting notes can be used as talking points during the assessment's Q&A part because they show diagnostic thinking and security knowledge.

C.3 Common Troubleshooting Scenarios

A straightforward test matrix aids in proving that the rules operate as intended.

Examples of tests are as follows:

Test 1: A-GUI → A-GW (HTTPS 443)

- Goal: confirm that management access is allowed.
- Anticipated: portal loads; log entry complies with the "Management HTTPS" requirement.

Test 2: ICMP ping from A-GUI to A-GW

- Goal: verify the troubleshooting rule (if activated).
- Anticipated: ping responses; log complies with the ICMP allow rule. Ping should fail and match cleanup drop if the ICMP rule is turned off.

Test 3: ClientS1 → Internet (HTTP/HTTPS) (if configured with an outgoing rule)

- Goal: verify user access to browsing (least-privilege allow).

- Expected: logs indicate the correct rule and web access functions.

Test 4: ClientS1 → Internet (FTP/Telnet) (explicit block)

- Goal: show how to avoid insecure protocols.
- Anticipated: connection failure; log shows drop by cleanup rule or "Block legacy protocols."

Test 5: Inter-site ClientL1 ÷ ClientS1

- Goal: verify segmentation choices.
- Expected: contingent upon the proposed design. Inter-site traffic ought to be prohibited if it is not necessary. Allow just the necessary ports and record the rationale if necessary (e.g., domain replication).
Select a minimum of one positive test and one negative test, then display the associated log entries during the demonstration. This supports your security argument with technical evidence.

C.2 Suggested Test Matrix (What to Test and Expected Result)

During the demonstration, the following checklist may be utilised:

1) Connectivity in Management

- Verify that you can access the GAIa portal for A-SMS (10.1.1.101) and A-GW (10.1.1.1) from A-GUI.
- Verify that SmartConsole can display objects and log in to A-SMS.

2) SIC Medical

- Go to Gateways & Servers → A-GW → Communication → Test SIC Status in SmartConsole.
- "Communicating" and building trust are anticipated.

3) Permissions

- Verify that licenses are attached and in the repository under SmartUpdate/Licence & Contracts.

- Verify that the license status and expiration fields are filled in in SmartConsole.

4) Enforcement of Policy

- Verify "Succeeded" after installing the policy to A-GW.

- Confirm the functionality of a permitted service (such as HTTPS management).

- Confirm that a blocked service (such as Telnet/FTP or other unauthorised traffic) is unsuccessful.

- Verify logs that demonstrate the activity and rule match.

5) Extra Features (if activated) Verify that the IPS and antivirus blades are available and enabled. • Verify the installation of the Threat Prevention policy, if any.

C.1 Validation Checklist

A systematic validation method and standard troubleshooting checks are provided in this appendix. Because incorrect setup might result in outages or security flaws, changes in business security operations must be confirmed after implementation. Here, the same discipline is used: each requirement is accompanied with proof and a test that may be repeated.

Appendix D – Documentation and Demonstration Notes

Conclusion

Check Point GAiA appliances were installed and centrally managed using A-SMS and SmartConsole to safeguard the enterprise network. Correct topology integration, steady management connectivity, effective SIC establishment, license handling via SmartUpdate, and the development of a default-deny firewall policy with specified management allowances are all demonstrated in this study. To better integrate the environment with accepted enterprise security requirements and to facilitate the lab's future growth, additional security measures were suggested. Overall, the configuration options match the assessment standards for secure enterprise network deployment by giving priority to least privilege, auditability, and maintainability.