



MODULE TITLE:
Enterprise Network Security

STUDENT NAME: MIZANUR RAHMAN

STUDENT ID: 2433477

COURSE: MSc Cybersecurity and Digital Forensics

LECTURER: Renuga Jayakumar

DATE OF SUBMISSION:

17th DECEMBER 2025

1 – Deployment of Centralized Security Management Infrastructure

1.1 Introduction

The purpose of Task 1 was to enhance the existing enterprise network topology developed in Part One by implementing a centralized security management architecture using Check Point Gaia appliances. In modern enterprise environments, managing security policies individually on gateways is inefficient and prone to misconfiguration. Centralized security management allows administrators to define, control, and audit security policies from a single point while maintaining consistent enforcement across the network.

To achieve this, a Check Point Security Management Server (A-SMS) running Gaia OS R81.20 was deployed alongside an existing Security Gateway (A-GW). A dedicated management workstation (A-GUI) was used to install and operate Check Point SmartConsole, which provides a graphical interface for managing gateways, policies, logs, and licenses.

All configurations were implemented in a controlled virtualized environment using Oracle VirtualBox, ensuring isolation and repeatability. The successful completion of this task establishes the foundational infrastructure required for implementing firewall rules and advanced security features in subsequent tasks.

1.2. Modification of Existing Topology

The original topology from Part One was extended to support centralized security management. Instead of managing firewall configurations locally on the gateway, a dedicated Security Management Server (A-SMS) was introduced. This modification aligns with enterprise best practices, where policy definition and enforcement are separated for better control and scalability.

The updated topology consists of the following components:

- **A-GW** – Check Point Security Gateway running Gaia OS, responsible for enforcing security policies.
- **A-SMS** – Check Point Security Management Server running Gaia OS, responsible for centralized policy management, logging, and monitoring.
- **A-GUI** – Management workstation used by the administrator to access SmartConsole.

The Oracle VirtualBox Manager confirms that all three virtual machines are deployed and running simultaneously, indicating that the topology modification was successful.

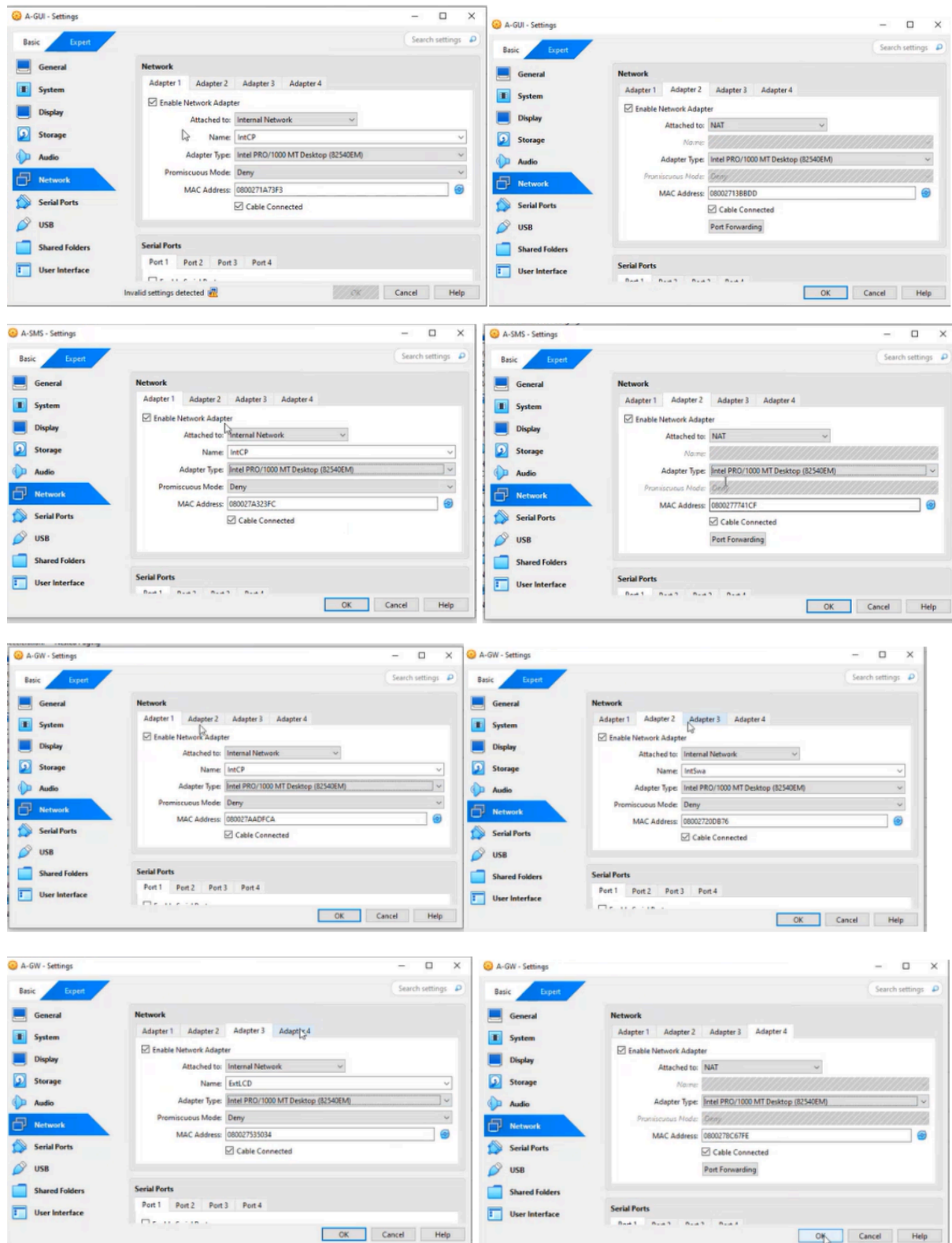


Fig-1 Oracle VirtualBox showing A-GW, A-SMS, and A-GUI running]

This screenshot demonstrates that the required infrastructure components are operational and ready for configuration.

1.3. Installation and Configuration of A-GW (Security Gateway)

i.Gaia OS Installation on A-GW

The **Check Point Gaia R81.20** operating system was installed on the A-GW virtual machine. During the installation process, disk partitions were allocated in accordance with system requirements to ensure adequate space for logs and future configurations.

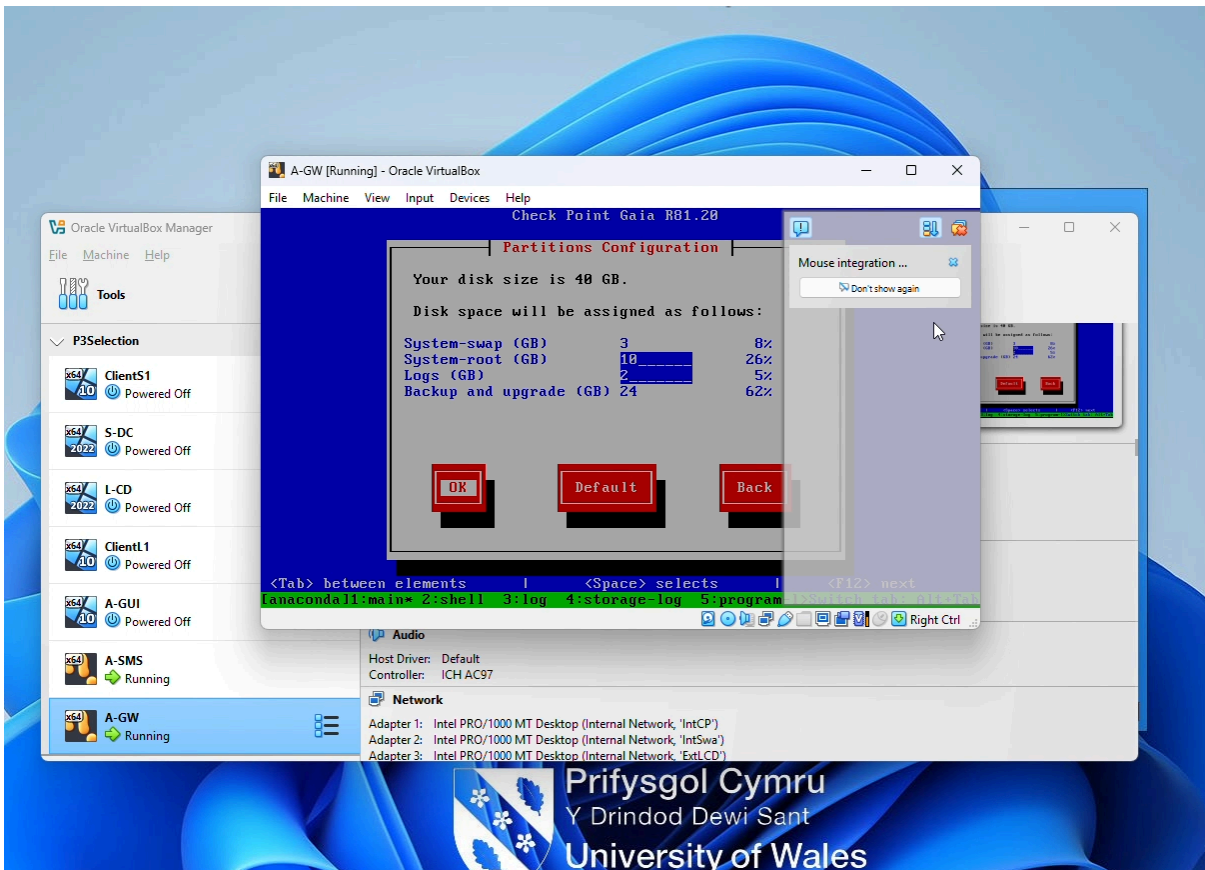


Fig- 2: Gaia installation – disk partition configuration (40 GB)]

This confirms that the gateway operating system was installed correctly and prepared for further configuration.

ii. Network Configuration of A-GW

After installation, the management interface (**eth0**) of the gateway was configured with a static IP address to enable stable communication with the Security Management Server.

Configured parameters were:

- **IP Address:** 10.1.1.1
- **Netmask:** 255.255.255.0
- **Default Gateway:** 10.1.1.254

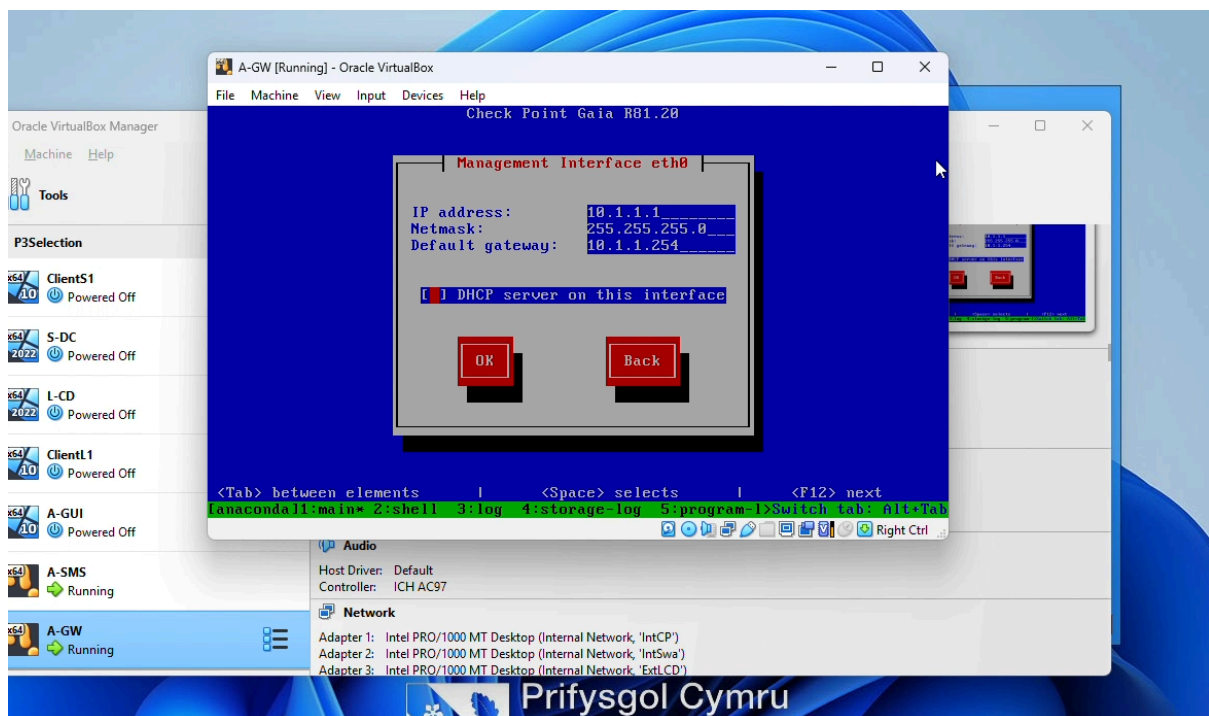


Fig 3: A-GW management interface IP configuration]

A static IP address was chosen because management and security infrastructure components require consistent addressing. Using DHCP could cause connectivity loss if the IP address changes, which would disrupt centralized management.

lii. Initial Gateway Access

Following network configuration, the gateway booted successfully and presented a console login prompt, indicating that the operating system was running correctly and ready for integration with the management server.

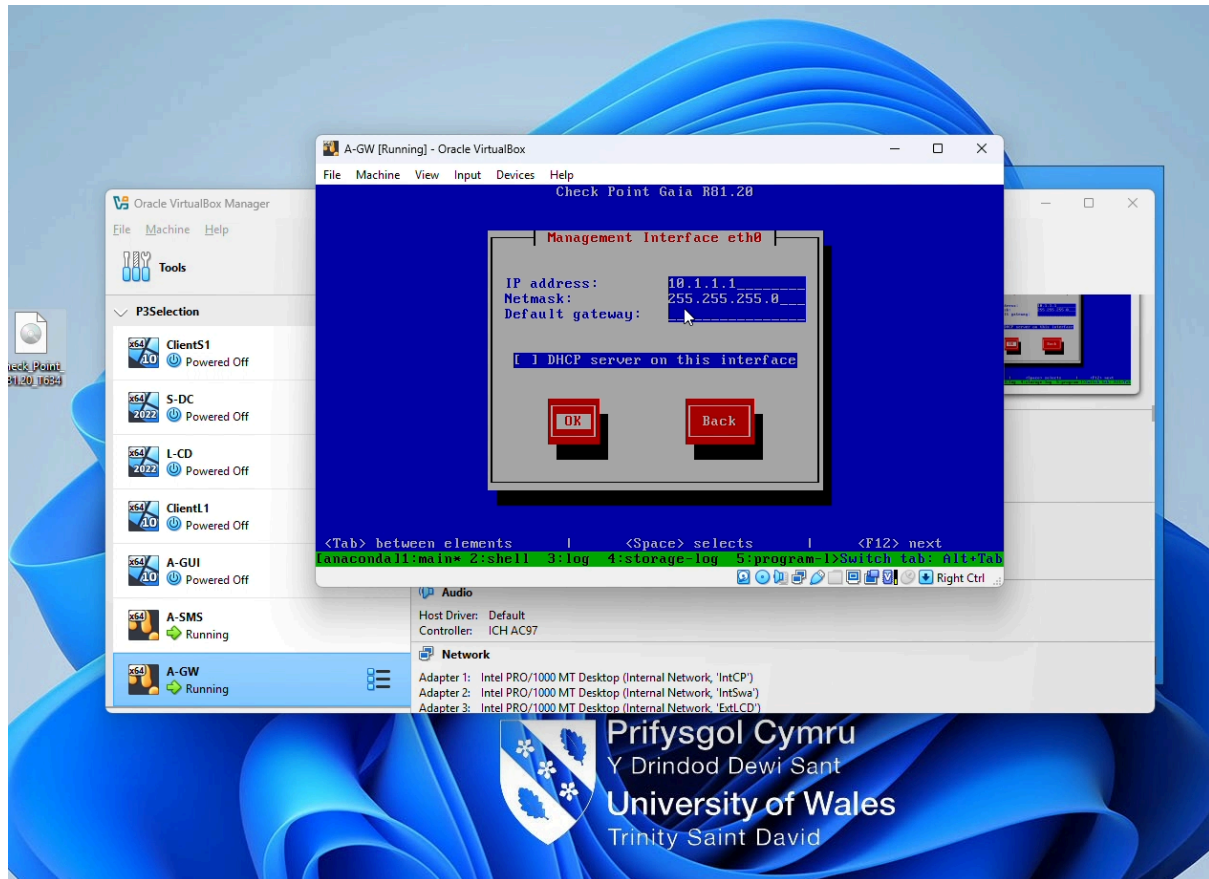


Fig 4: A-GW console login prompt]

This confirms that the gateway is operational and ready to be managed via SmartConsole.

1.4. Installation and Configuration of A-SMS (Security Management Server)

I. Gaia OS Installation on A-SMS

The same Gaia R81.20 operating system was installed on the A-SMS virtual machine to maintain version compatibility with the gateway. Version consistency is important in Check Point environments to avoid management or policy deployment issues.

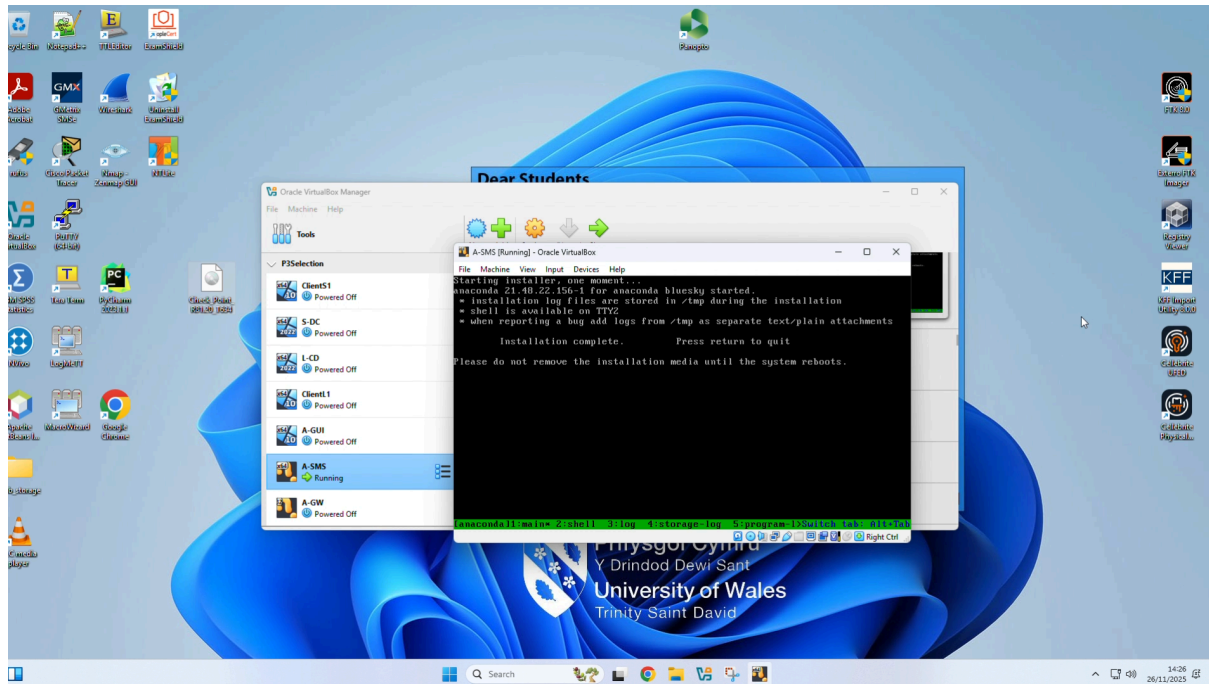


Fig-5: A-SMS installation completion screen]

This screenshot verifies that the Security Management Server installation completed successfully.

ii Network Configuration of A-SMS

The management interface of A-SMS was configured with a static IP address to allow reliable connectivity from SmartConsole and managed gateways.

Configured parameters were:

- **IP Address:** 10.1.1.101
- **Netmask:** 255.255.255.0

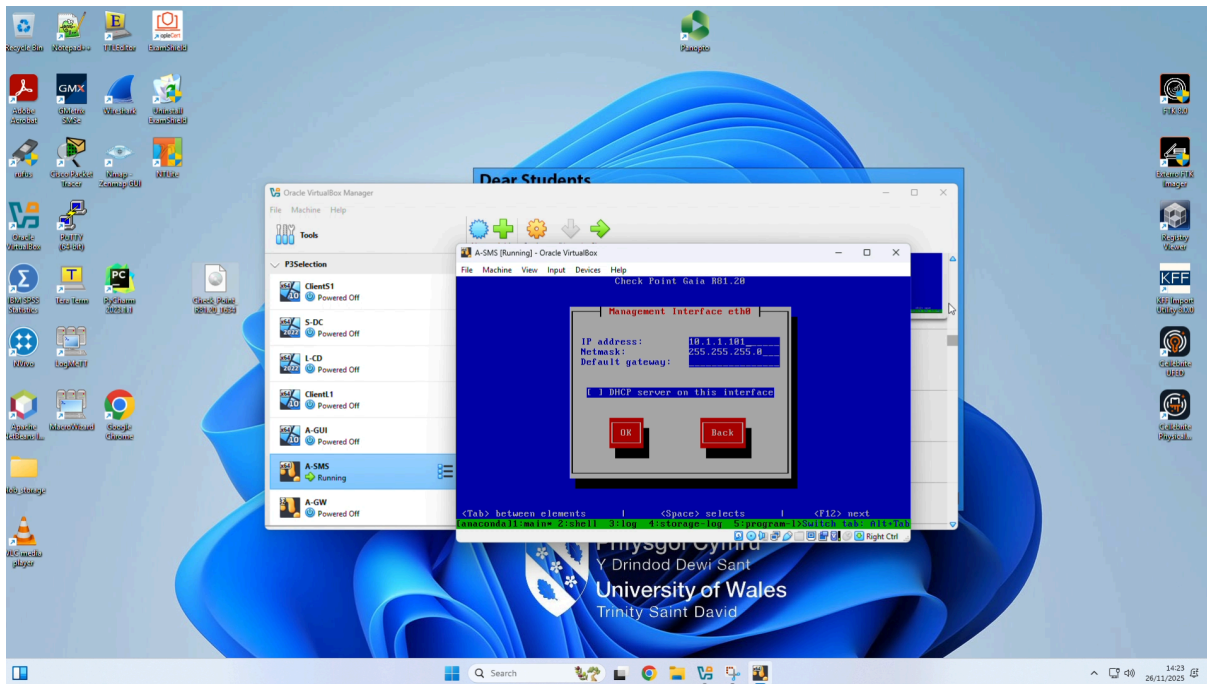


Fig- 6: A-SMS network/IP configuration]

This IP address serves as the central point for administrative access and is used by SmartConsole to connect to the management server.

1.5. Installation and Use of A-GUI (SmartConsole)

SmartConsole **R81.20** was installed on the management workstation (A-GUI). SmartConsole is the primary administrative tool used in Check Point environments to manage gateways, define security policies, monitor logs, and apply licenses.

i. SmartConsole Login

SmartConsole was configured to connect to the Security Management Server using its static IP address.

Login details included:

- **Management Server:** 10.1.1.101
- **Administrator account:** Valid management credentials

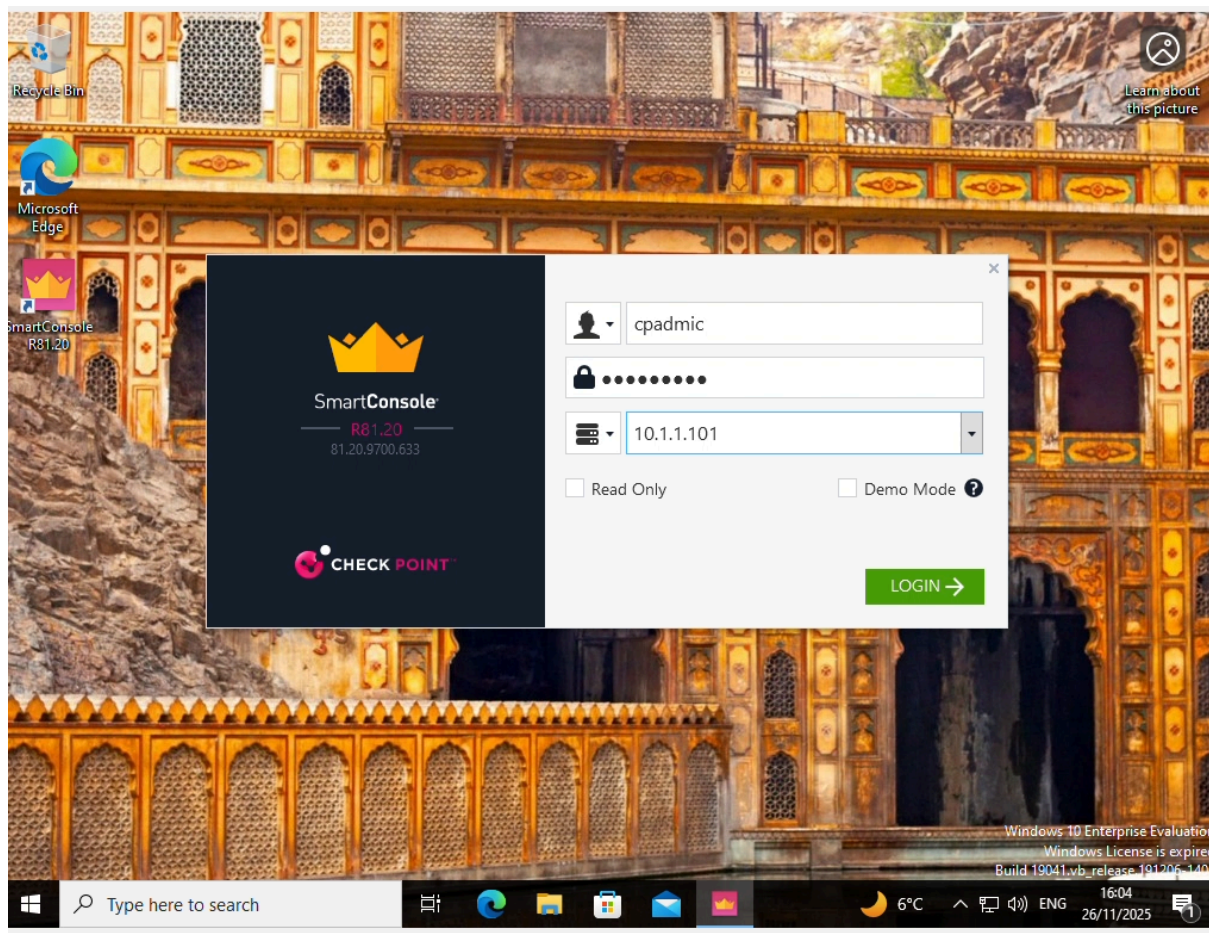


Fig- 7: SmartConsole login screen connected to 10.1.1.101]

Successful login confirms that A-GUI can communicate securely with A-SMS and that centralized management is functioning.

1.6. Adding and Configuring the Security Gateway in SmartConsole

i. Gateway Object Creation

The **Check Point Gateway Installation Wizard** was used within SmartConsole to add the A-GW as a managed gateway.

Configured details:

- **Gateway Name:** A-GW
- **Platform:** Open Server
- **IPv4 Address:** 10.1.1.1

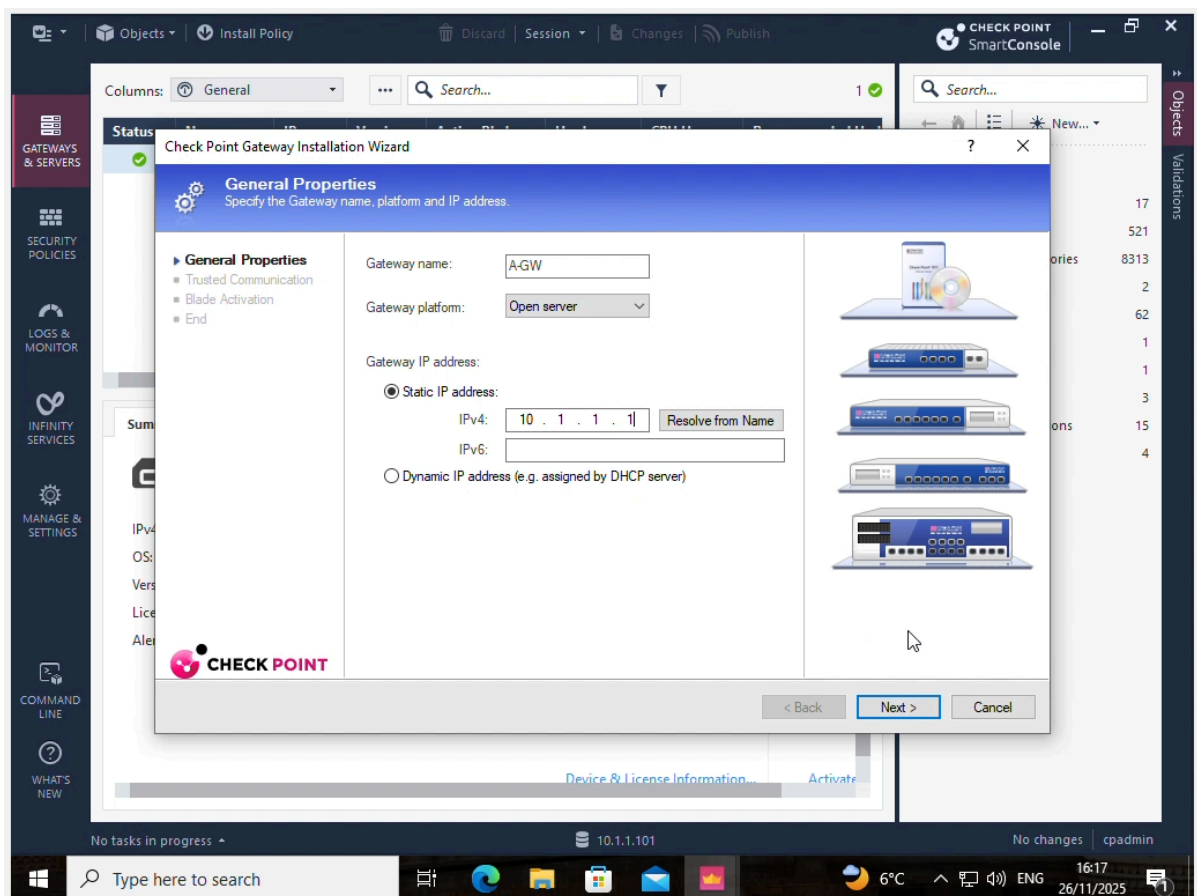


Fig- 8: Gateway Installation Wizard – General Properties]

This step formally registers the gateway with the management server.

ii. Secure Internal Communication (SIC)

Secure Internal Communication (SIC) was established between A-SMS and A-GW. SIC provides encrypted, certificate-based trust between management and gateway components.

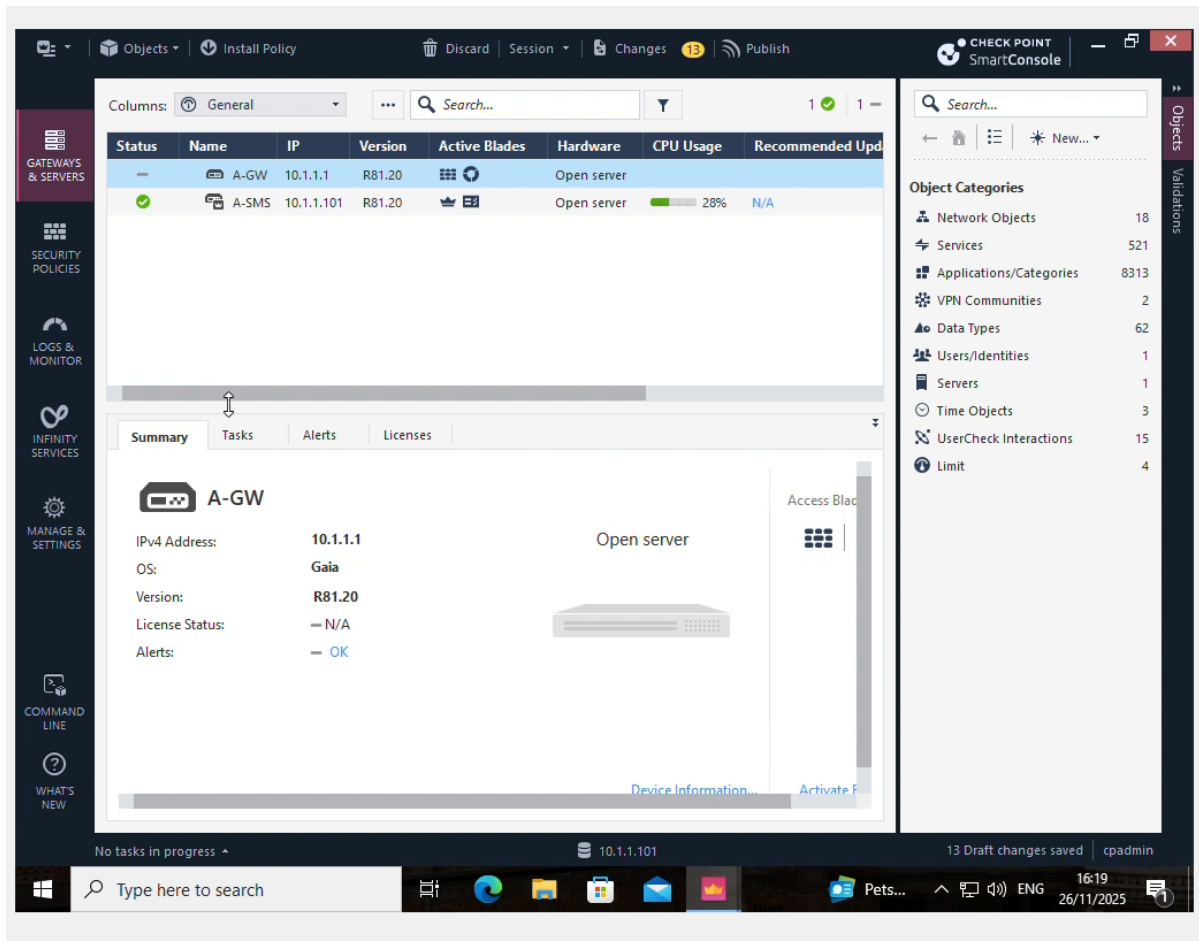


Fig-9: SIC / Trusted Communication topology retrieval]

The topology retrieval confirms that the management server can communicate with the gateway and detect all configured interfaces.

lii. Gateway Installation Completion

The installation wizard completed successfully, confirming:

- SIC trust established
- Firewall and NAT blades enabled

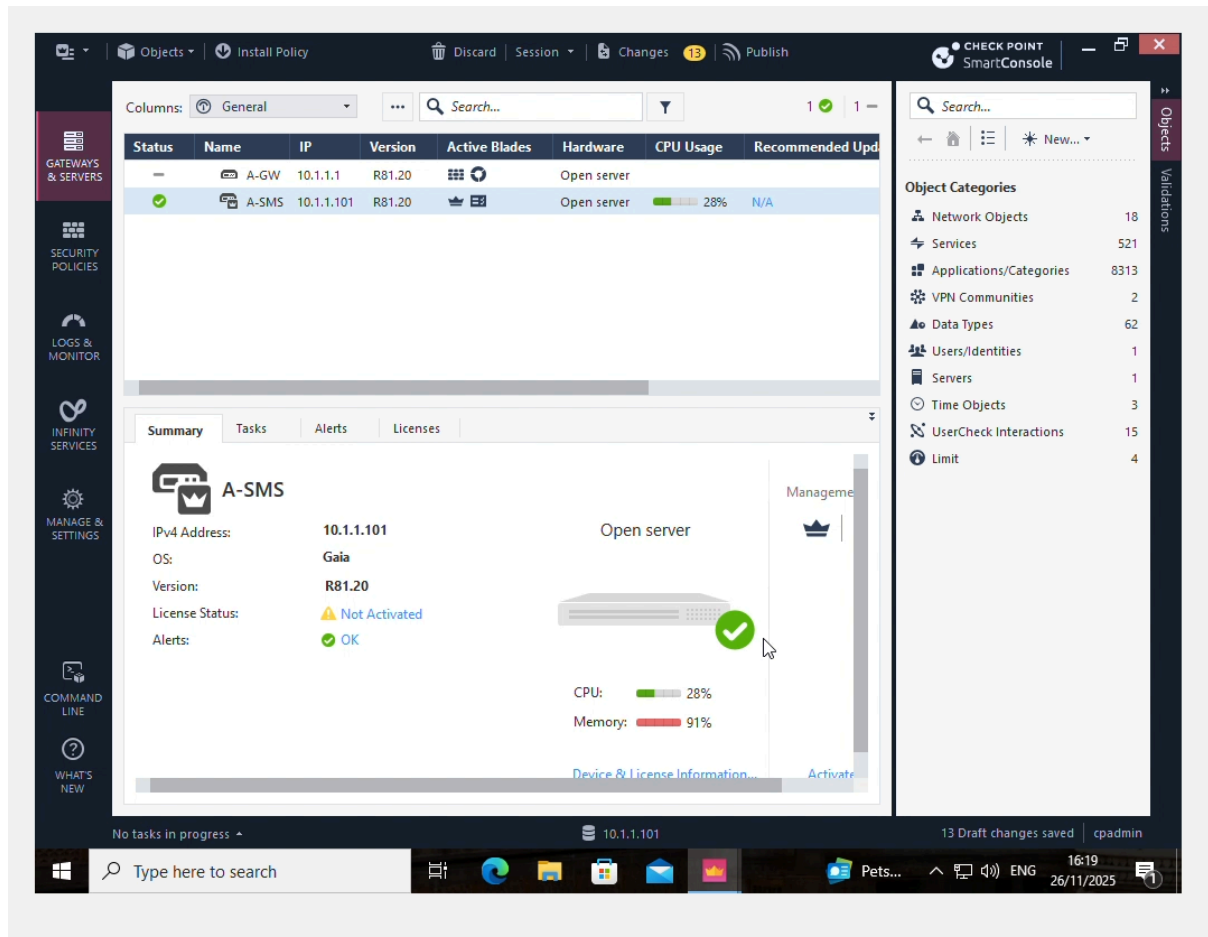


Fig-10: Gateway Installation Wizard completion summary]

This indicates that the gateway is fully integrated into centralized management.

iv. Gateway Properties Verification

Gateway properties were reviewed to ensure:

- Correct IP address
- Correct platform and version (R81.20)
- SIC status showing **Trust established**

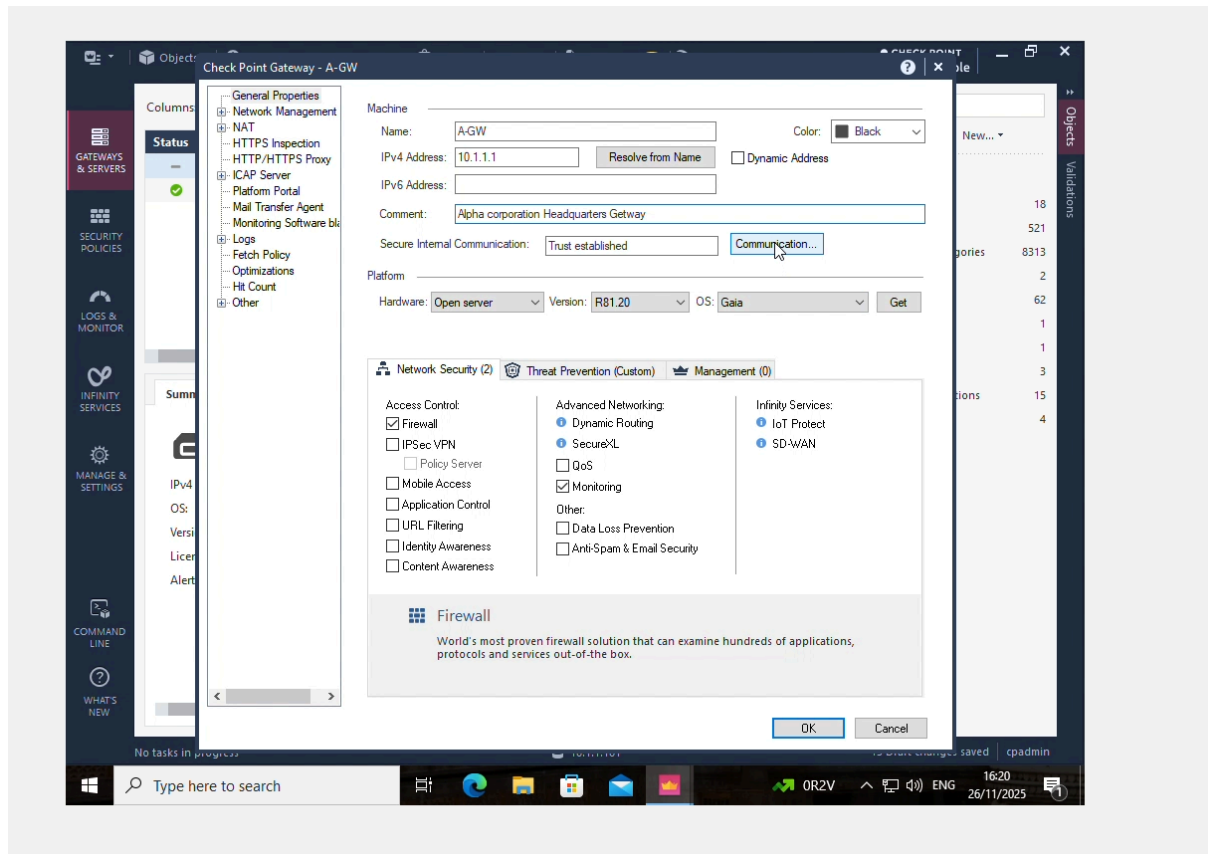


Fig- 11: A-GW properties showing Trust established]

This verification step ensures that the gateway is ready to receive policies from A-SMS.

1.7. Licensing of SMS and Gateway

Licensing was applied using **SmartConsole / SmartUpdate** in accordance with Check Point guidelines.

I. License Attachment Confirmation

License files were added and successfully attached to the Security Management Server and the Security Gateway

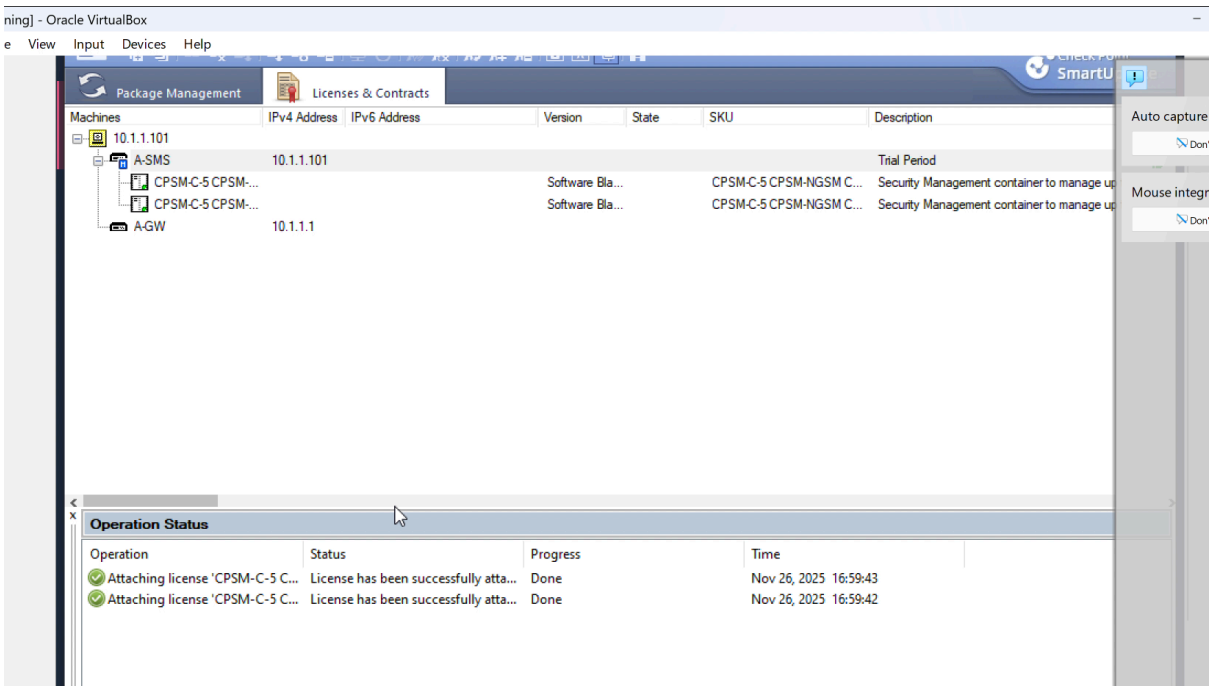


Fig-12: SmartUpdate / License attachment success status]

This confirms that licensing was applied correctly.

ii. License Status Verification

The licensing status of both A-SMS and A-GW was verified from the **Gateways & Servers** view in SmartConsole.

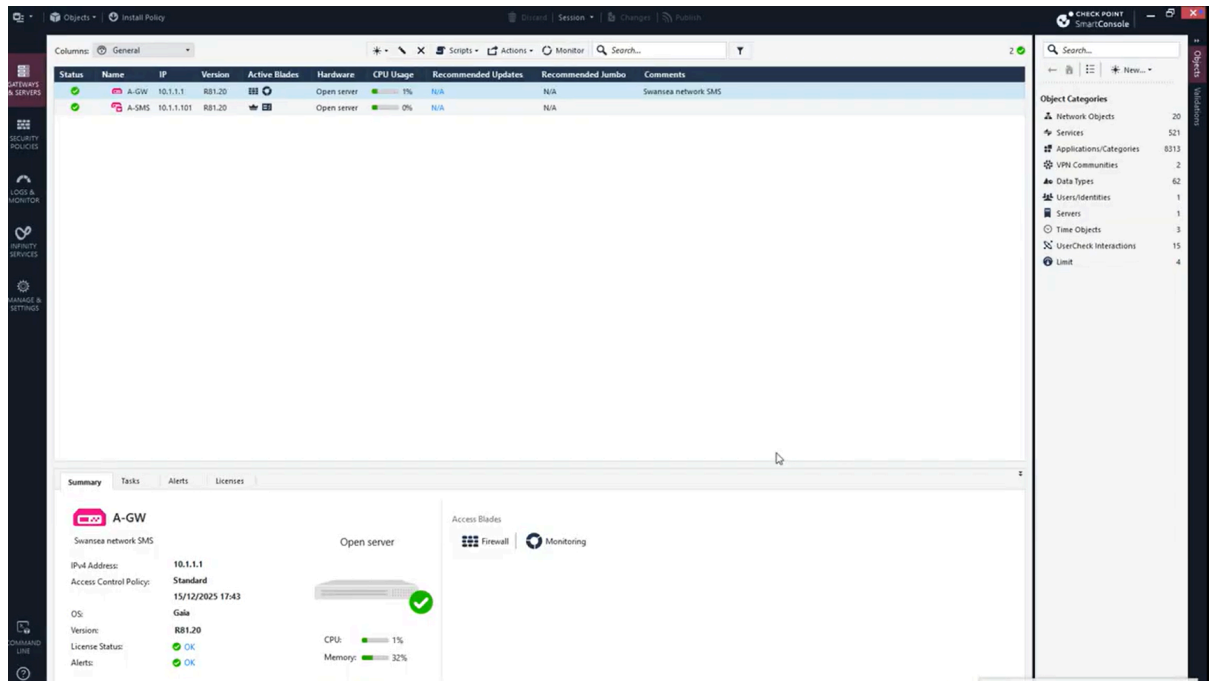


Fig- 13: Gateways & Servers view showing license status OK]

This confirms that the deployed systems meet the module and licensing requirements for operation.

1.8. Publishing Configuration Changes

After completing all configurations, changes were published within SmartConsole to commit them to the management database.

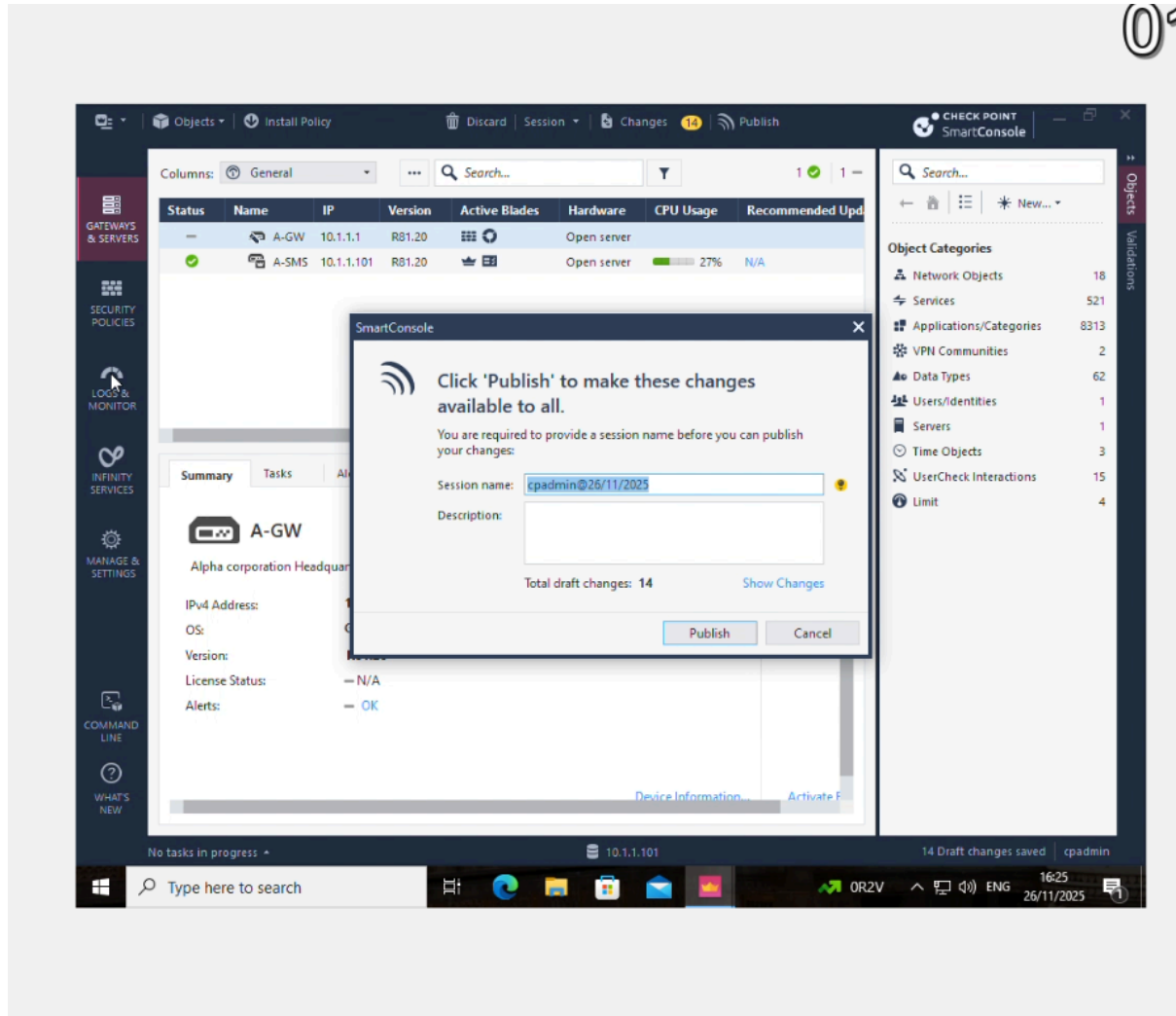


Fig- 14: SmartConsole “Publish” confirmation]

Publishing ensures that all configuration changes are active and consistent across the environment.

1.9. Verification of Connectivity (Swansea Network ↔ A-SMS)

Connectivity between the Swansea Network components and the Security Management Server was verified by reviewing the status indicators in SmartConsole.

Observed indicators included:

- Green status icons
- No system alerts
- Normal CPU and memory usage

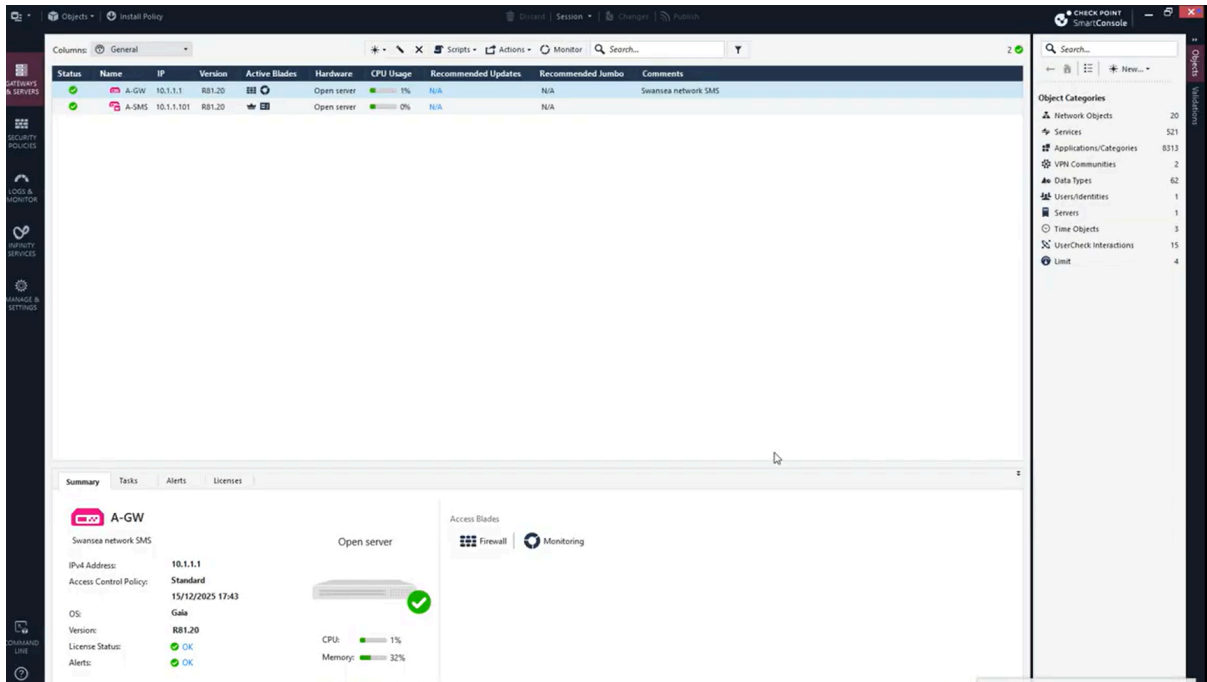


Fig- 15: Gateways & Servers showing green status for A-SMS and A-GW]

This confirms that centralized management communication is stable and operational.

2– Firewall Rule Definition, Enforcement, and Demonstration.

2.1 Objective

The objective of Task 2 is to design, implement, enforce, and demonstrate firewall rules that regulate both inbound and outbound traffic within the enterprise network, based on a realistic and practical enterprise security policy. The firewall rules were configured and centrally managed using Check Point SmartConsole, which enables administrators to define policies, deploy them consistently across gateways, and monitor enforcement through logging and status indicators.

Rather than relying on default or permissive configurations, this task focuses on explicit traffic control, policy justification, and practical verification of enforcement. Each firewall rule was deliberately tested by first allowing traffic and then blocking the same traffic to confirm that the security gateway correctly enforces policy changes only after they are published and installed. This mirrors how firewall policies are validated in real enterprise environments.

The overall firewall policy follows the principle of least privilege, ensuring that only services required for management, diagnostics, and controlled operations are permitted, while all other traffic is denied by default through an explicit cleanup rule.

2.2 Enterprise Security Policy (Justification)

In enterprise environments, firewalls serve as the primary enforcement mechanism that separates trusted internal systems from potentially untrusted networks. Weak or poorly structured firewall policies often result in unintended exposure of services, increased attack surfaces, and difficulty in auditing security posture.

To mitigate these risks, the firewall policy implemented in this task was designed according to the following enterprise security principles:

Restricted Administrative Access (SSH)

Administrative services such as SSH provide direct access to critical infrastructure components, including the security gateway itself. If left unrestricted, SSH can be exploited through brute-force attacks, credential compromise, or unauthorized administrative access. For this reason, SSH access was restricted to authorized management systems only and explicitly tested to ensure that unauthorized access attempts are blocked.

Controlled Diagnostic Access (ICMP)

ICMP traffic is essential for basic connectivity testing and troubleshooting, particularly during deployment and fault diagnosis. However, unrestricted ICMP can be abused for network reconnaissance, host discovery, and traffic analysis. As a result, ICMP was selectively permitted and tested to confirm that diagnostic functionality remains available without exposing the network to unnecessary probing.

Limited File Transfer Services (FTP)

File transfer protocols can pose significant risks if not properly controlled, as they may be used to exfiltrate sensitive data or introduce malicious files into the network. In enterprise environments, such services should be restricted to trusted systems and monitored closely. FTP access was therefore limited and explicitly tested to demonstrate both allowed and blocked behavior.

Explicit Default Deny Policy

A fundamental principle of secure firewall design is that any traffic not explicitly permitted should be denied. Relying on implicit allow behavior can lead to unintentional access paths and security gaps. To prevent this, a cleanup rule was implemented at the end of the policy to explicitly drop all unspecified traffic.

This security approach aligns with recognized standards and best practices, including:

- **ISO/IEC 27001**, which emphasizes controlled access to information systems
 - **NIST SP 800-53**, which mandates least privilege and boundary protection
 - **Check Point security best practices**, which recommend explicit allow rules followed by a default deny strategy
-

2.3 Firewall Rules Configuration

Firewall rules were configured within the **Access Control Policy** in SmartConsole. Rule order was carefully maintained to ensure correct top-down evaluation, as firewall rules are processed sequentially.

Rule	Traffic Type	Source	Destination	Action	Purpose
1	SSH	A-GUI	A-GW	Allow / Drop (tested)	Controlled administrative access
2	ICMP (Ping)	A-GUI	A-GW	Allow / Drop (tested)	Network diagnostics
3	FTP	A-GUI	SDC	Allow / Drop (tested)	Secure file transfer
4	Cleanup Rule	Any	Any	Drop	Block all other traffic

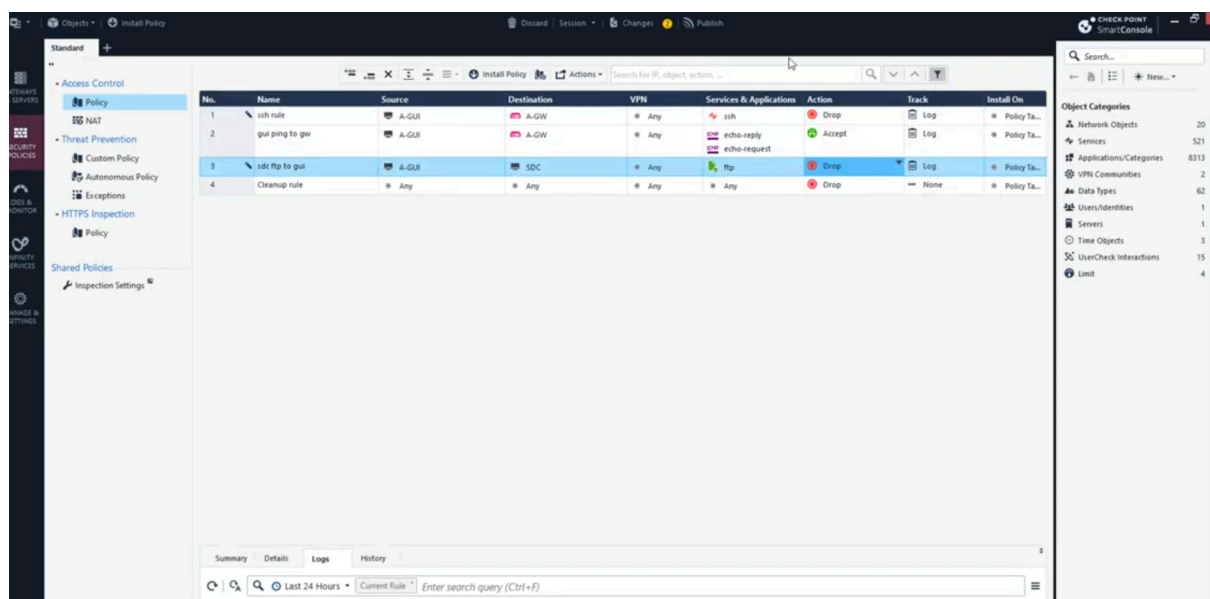


Fig-16 :Access Control Policy Showing SSH, ICMP, FTP and Cleanup Rules

This screenshot confirms that the firewall policy is explicitly defined, includes only required services, and enforces a **default-deny strategy** using a cleanup rule at the bottom of the policy.

2.4 SSH Traffic Control (Inbound & Outbound)

SSH access to the security gateway was configured to demonstrate both **authorized access** and **unauthorized access blocking**, reflecting real-world administrative control practices.

When the SSH rule was configured to **Allow**, an SSH connection attempt from the authorized management workstation successfully reached the authentication stage. This confirms that the firewall permitted the traffic and forwarded it to the gateway service as intended.

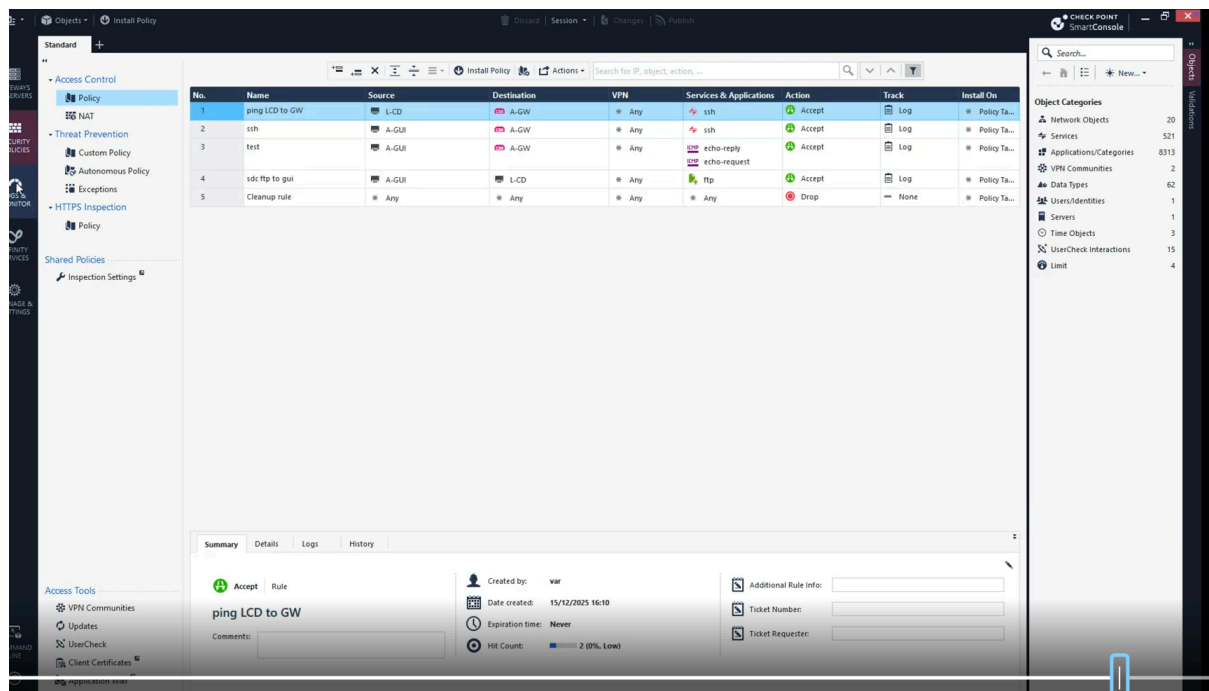


Fig-17 :SSH Access Allowed – Authentication Prompt Displayed

To validate enforcement, the SSH rule action was then modified to **Drop**, followed by publishing and installing the updated policy. After the policy was applied, subsequent SSH connection attempts resulted in a connection timeout, confirming that the firewall actively blocked unauthorized access at the network level.

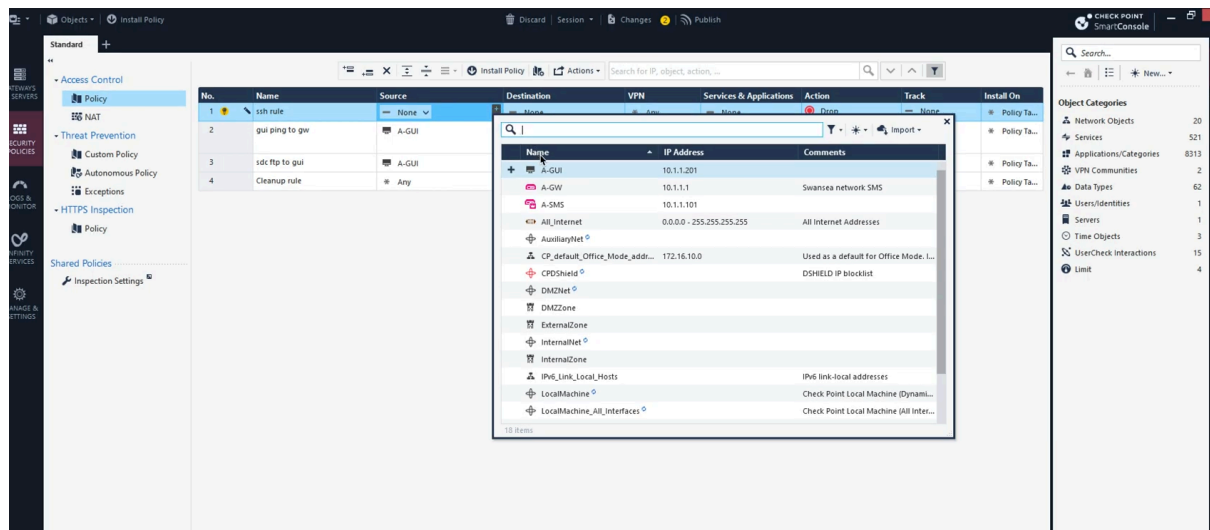


Fig-18 :SSH Rule Modified to Drop Unauthorized Access

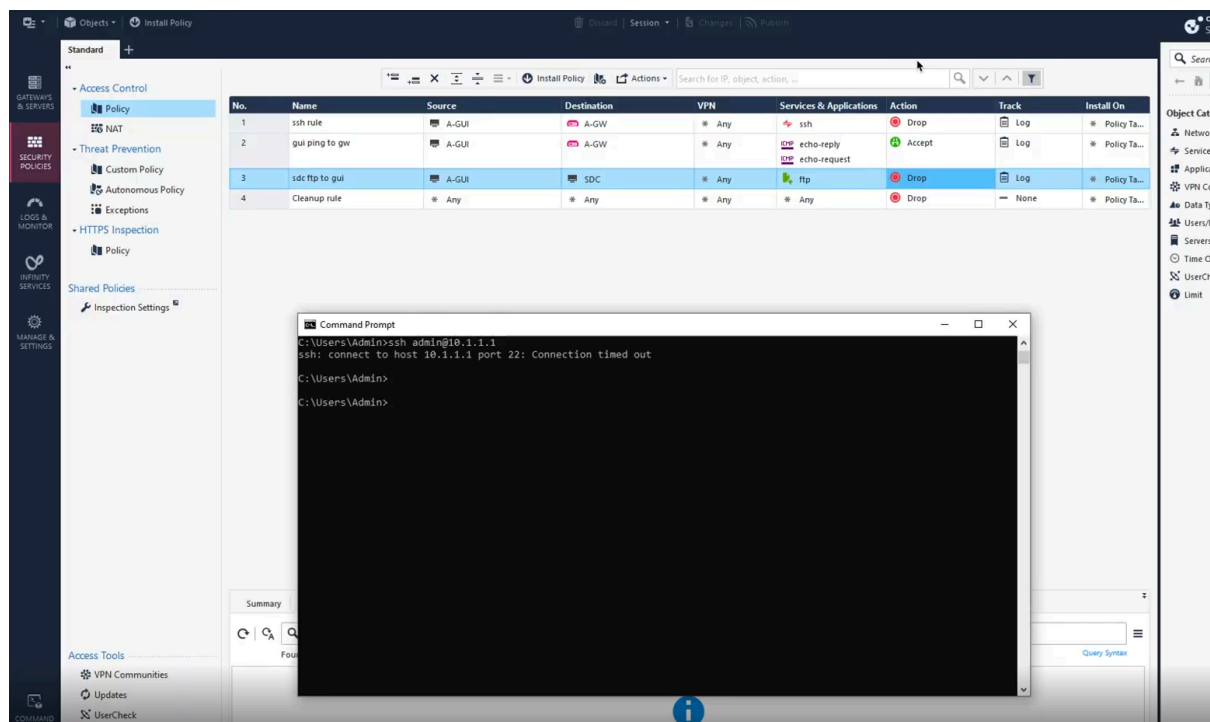


Fig-19 : SSH Traffic Blocked – Connection Timeout Observed

This process demonstrates that firewall rule changes only take effect after proper publication and installation, which aligns with enterprise change management and control procedures.

2.5 ICMP (Ping) Traffic Control

ICMP traffic was selectively permitted to support network diagnostics while maintaining overall security.

When ICMP was allowed, echo-request and echo-reply packets successfully traversed the firewall, confirming connectivity between the management workstation and the security gateway.

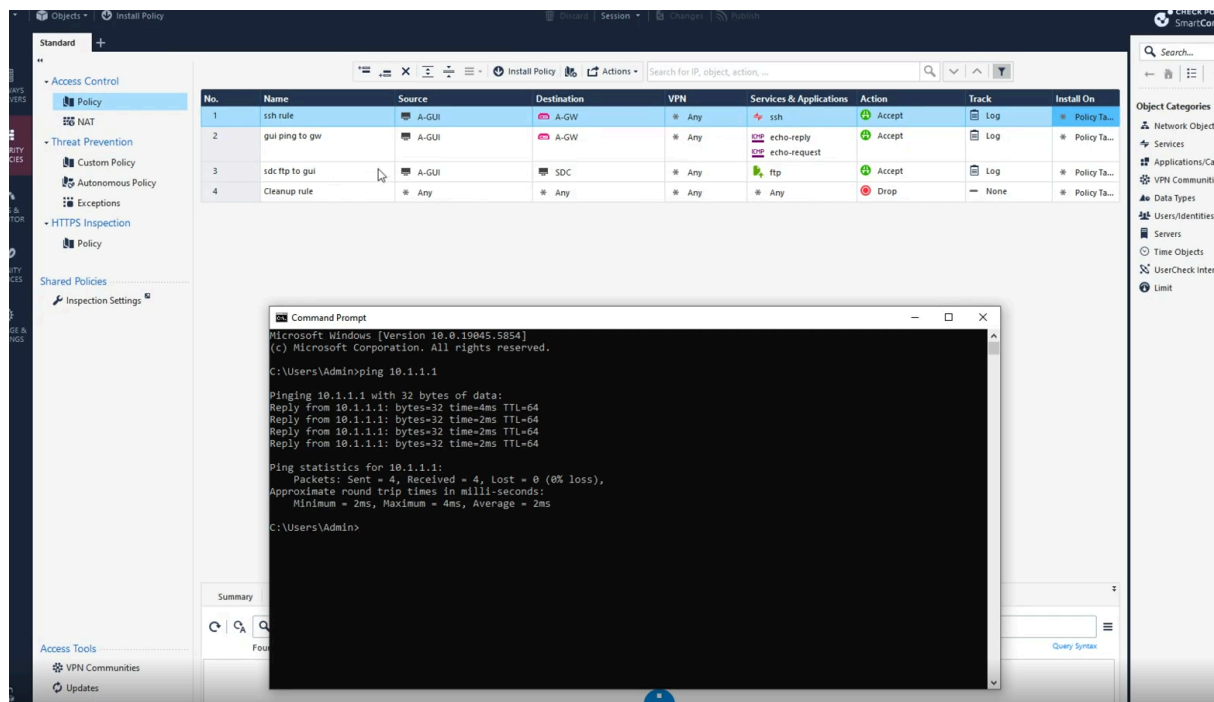


Fig-20 :ICMP Traffic Allowed – Successful Ping Test

This controlled configuration ensures that diagnostic capabilities remain available to administrators without exposing the network to unnecessary reconnaissance traffic.

2.6 FTP Traffic Control

FTP access was configured to allow file transfer only between trusted systems. This reflects enterprise environments where file transfer services are strictly regulated and monitored to prevent data leakage or malware introduction.

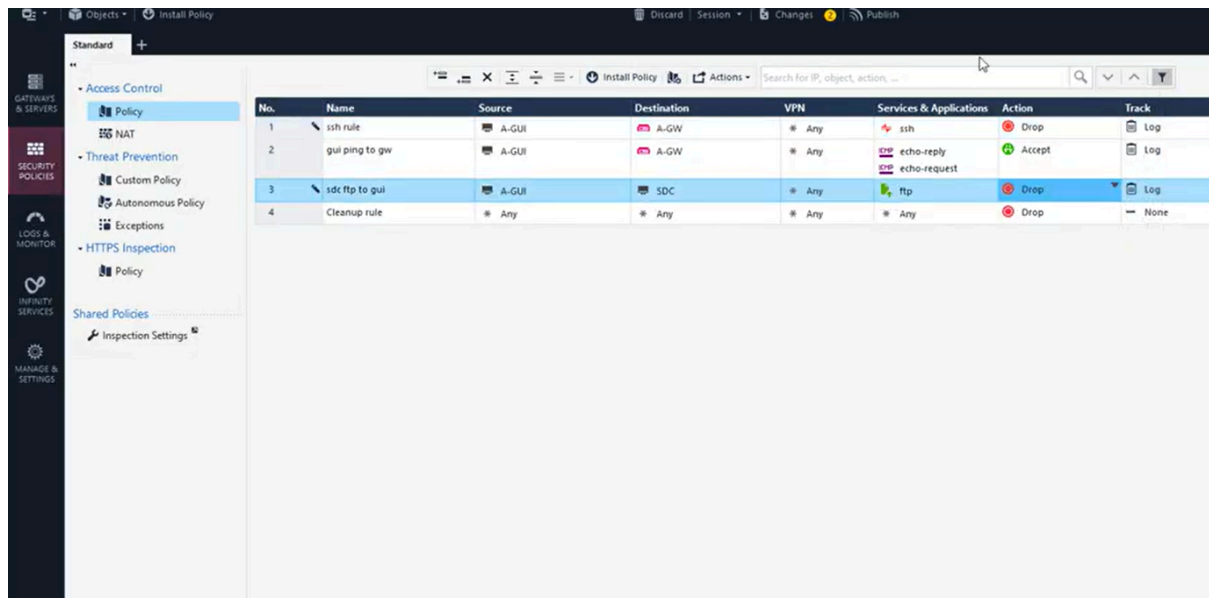


Fig-21 :FTP Traffic Control Rule Configuration

After modifying the FTP rule action to **Drop** and installing the policy, FTP traffic was successfully blocked. This confirms that the firewall correctly enforced the updated policy and prevented unauthorized file transfers.

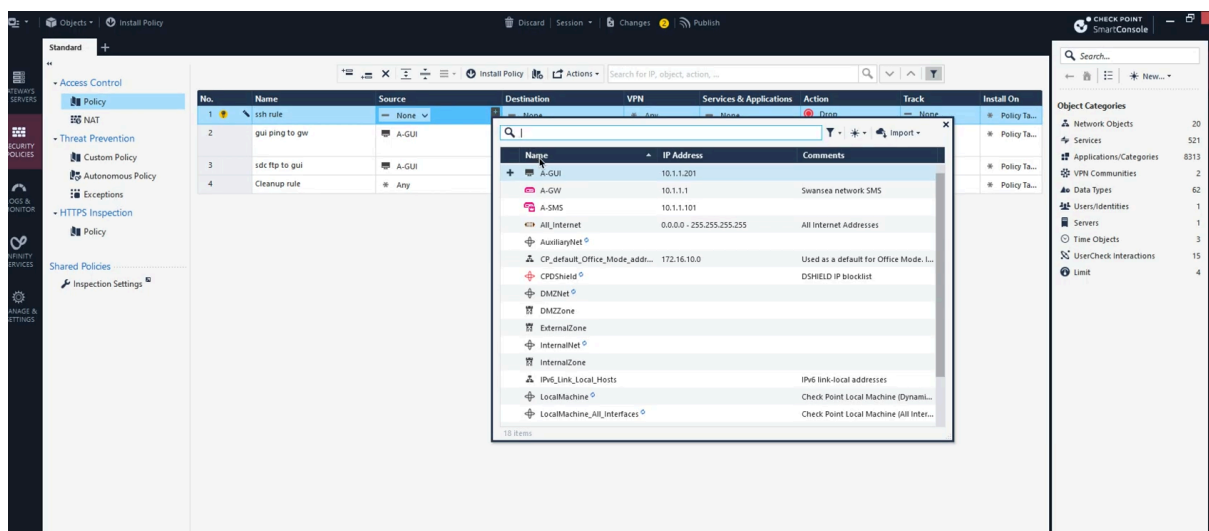


Fig-22 :FTP Traffic Blocked by Firewall Policy

This test demonstrates the firewall's ability to dynamically enforce access restrictions based on policy changes.

2.7 Cleanup Rule Enforcement

A cleanup rule was placed at the bottom of the Access Control Policy to explicitly drop all traffic that does not match any preceding rule.

The cleanup rule ensures:

- No implicit allow behavior
 - Reduced exposure to unknown or unexpected traffic
 - Clear policy completeness and predictability
-

2.8 Policy Installation and Logging

After each policy modification:

- Configuration changes were published
- The updated policy was installed on A-GW
- Logs were reviewed to verify both accepted and dropped traffic

Policy installation ensures that configuration changes are actively enforced by the gateway and provides traceability for auditing and security review purposes.

3– Additional Security Features Using Gaia Appliances

3.1 Objective

The objective of Task 3 is to enhance the enterprise network's security posture by implementing **additional security controls** aligned with recognized industry standards and Check Point guidelines. These enhancements focus on strengthening administrative access, ensuring centralized management, and improving visibility through monitoring and logging.

3.2 Administrative Access Control

Administrative access was strengthened by configuring administrator accounts with:

- Defined authentication methods
- Role-based permissions
- Account configuration policies

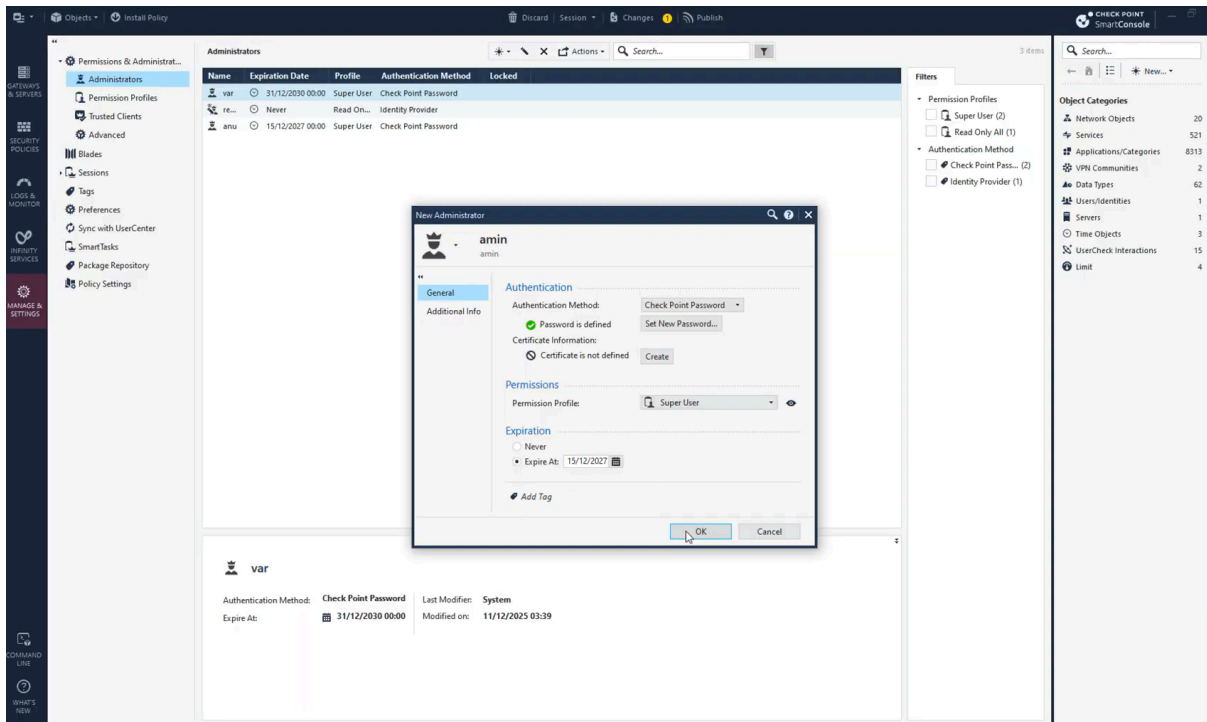


Fig-23 :Administrator Account and Role Configuration

This ensures that only authorized users can perform security management tasks and that administrative actions are accountable.

3.3 Centralized Policy Management

A dedicated **Security Management Server (SMS)** was used to centrally manage gateways, policies, and system health.

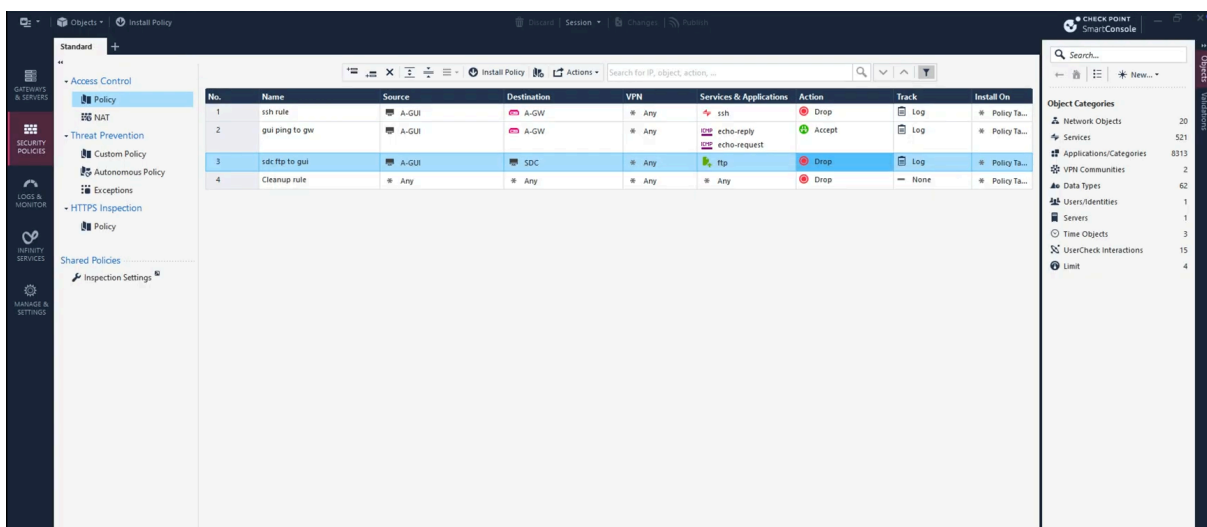


Fig-24 :Gateway and SMS Status Showing Successful Connectivity

Centralized management improves consistency, reduces configuration errors, and supports scalable enterprise operations.

3.4 Policy Change Management and Publishing

All configuration changes followed a controlled workflow involving:

- Session tracking
- Publishing changes
- Installing policies

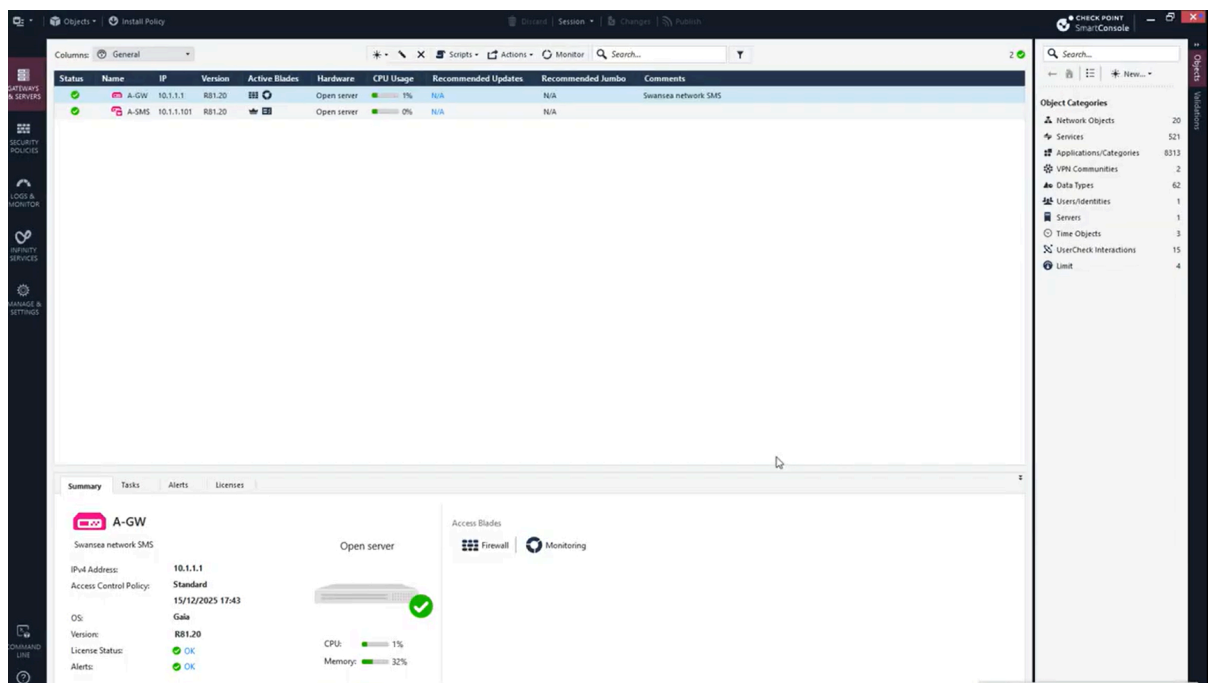


Fig-25 :Publishing Security Policy Changes

This aligns with enterprise change management practices and ensures traceability.

3.5 Monitoring, Logging, and Auditing

Logging was enabled for:

- Allowed traffic
- Blocked traffic
- Administrative actions

These logs provide visibility into firewall behavior and support security monitoring, compliance, and incident response.

3.6 Security Benefits Achieved

The implemented security features result in:

- Strong control over inbound and outbound traffic
 - Reduced attack surface
 - Improved compliance with enterprise security standards
 - Real-time visibility into network activity
-

4. Conclusion

This assignment successfully demonstrates the deployment and securing of an enterprise network using Check Point Gaia appliances in a centralized management architecture. Through the completion of Part 1, a robust foundation was established by introducing a dedicated Security Management Server (A-SMS), integrating it with the Security Gateway (A-GW), and managing the environment through SmartConsole installed on the management workstation (A-GUI). The use of centralized management reflects real-world enterprise practices, enabling consistent policy enforcement, simplified administration, and improved visibility across the network.

In Part 2, firewall rules were carefully designed and enforced based on realistic enterprise security requirements. By applying the principle of least privilege, only essential services such as SSH, ICMP, and FTP were selectively permitted, while all other traffic was explicitly denied through a cleanup rule. Each rule was practically validated by testing both allowed and blocked scenarios, ensuring that policy enforcement was functioning as intended after publication and installation. This approach highlights the importance of not only configuring firewall rules, but also verifying their effectiveness through live testing and logging.

Part 3 further enhanced the security posture of the enterprise network by implementing additional security controls aligned with industry standards and Check Point best practices. Administrative access was strengthened through defined roles and permissions, centralized policy management was reinforced via the Security Management Server, and policy changes followed a controlled publish-and-install workflow. Logging and monitoring capabilities provided visibility into both traffic flow and administrative actions, supporting auditing, troubleshooting, and incident response.

Overall, the implemented solution demonstrates a realistic and enterprise-grade security deployment. The combination of centralized management, strict firewall enforcement, controlled administrative access, and continuous monitoring significantly reduces the attack surface and improves the reliability and security of the network. This assignment reflects practical skills in deploying, managing, and securing enterprise networks using Check Point Gaia appliances and provides a solid foundation for advanced network security implementations.