



University of Wales Trinity Saint David

**Department of Cyber Security and Digital Forensics
Master's Programme**

Module: ACCA7032 –Enterprise Network Security

**Assignment Title: Applied Network Security: Contemporary Research, Practical Work,
and Demonstrations of Principles and Practices**

Name:

Md Mahfuzur Rahman

ID:

2431582

Submission Date:

17 December 2025

Part 1– Securing the Enterprise Network

Implementation of a Network Security Solution using Check Point Gaia

1. Introduction

Enterprise networks are faced with an escalating level of diverse threats that is constantly changing, from external cyber-attackers to internal sources such as mis-configuration, privilege abuse and insider attacks. Therefore, organizations need strong centrally managed security profile that blocks unauthorized access and offers visibility and easy policy enforcement in the process. Modern firewall solutions must provide more than just basic packet filters and instead facilitate a policy centralisation, secure administrative communication, logging of configuration changes in great detail and also allow for scalable enforcement policies that grow with the business over time or based on new risk priorities.

8D Report1 Introduction The following 5 pages are a report from the 3rd semester Final Project, for building an that demonstrates how to build and test and enterprise class Firewall (Check Point Gaia) within a simulated enterprise network. Following on from the initial topology defined in Part One, Part Two elaborated on measures to enhance the overall security posture of the network including how it approached centralised security management, secure egress via a multi-interface firewall gateway and enforcing consistent access control policies. Secure, centralized management was facilitated using SmartConsole, allowing policy setup, monitoring and verification from one management console. All design and configuration choices were validated through reference to established enterprise security best practices so that the proposed solution does not only satisfy functional requirements, but also complies with operational and governance standards of daily operations.

2. Updated Enterprise Network Architecture

To enhance the security posture of the enterprise network developed in Part One, the topology was extended to include dedicated Check Point security components. The final architecture consists of:

- **A-SMS:** Security Management Server (Gaia R81.20)
- **A-GW:** Security Gateway enforcing security policies
- **A-GUI:** Management workstation running SmartConsole
- Segmented **management**, **internal**, and **external** networks

This architecture supports separation of duties, reduces the attack surface, and enables consistent security policy enforcement across the enterprise.

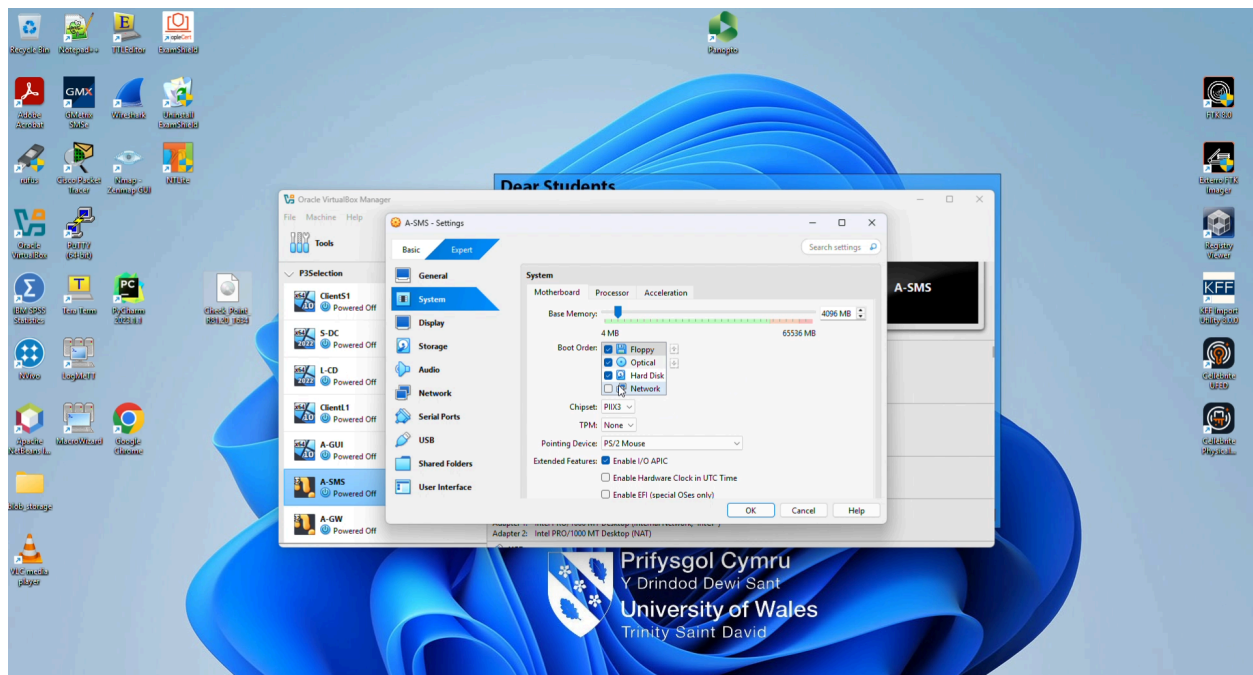


Figure 1: Updated enterprise network topology

3. Security Management Server (A-SMS) Configuration

3.1 Virtual Machine Preparation

The A-SMS virtual machine was created matching Check Point's recommended hardware and platform requirements to provide optimal performance and operational longevity. This involved setting up an appropriate amount of system memory for policy compilation, logging and management tasks, making sure the appliance is using 64-bit architecture so that it will be compatible with the Gaia OS, and configuring a separate mgmt network interface to segregate administrative traffic from user plane/data-plane traffic.

BladeLogic SecurityHardeningManager from BMC Software is a widely used enterprise-grade security policy and configuration management product that requires proper resource allocation to ensure it functions effectively. By complying with vendor-recommended settings, A-SMS offers consistent, centralized policy enforcement, accurate event correlation and dependable communication with managed security gateways. Accordingly, this configuration scales to satisfy policy complexity, capacity logging and security monitoring needs for the management infrastructure as these grow over time while maintaining high performance levels.

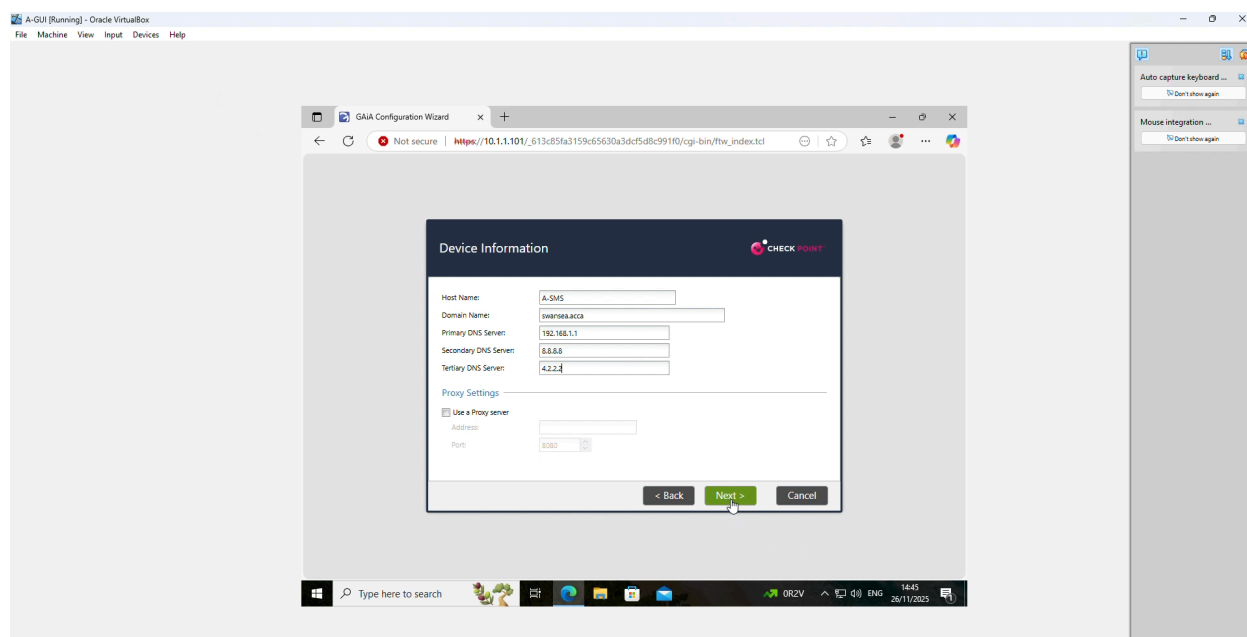


Figure 2: A-SMS VirtualBox hardware configuration

3.2 Gaia OS Installation and Initial Configuration

Check Point Gaia R81.20 was deployed on the Check Point Security Management Server (A-SMS) appliance in accordance with Check Point recommended installation process and best practices. While it was installing I setup a strong admin password for the management system, to protect against unauthorized administrative compromise of the management system. Management A static IP address was assigned for the Manage Traffic to and from A-SMs, Security Gateway, and SmartConsole management station.

DNS and NTP were set also up in the beginning setup. Reliable time synchronisation is very important in enterprise security environment because it provides correct log timestamps, facilitates consistent event correlation over more than one device and forms the basis for thorough incident investigation and auditing. By working together, these configuration settings lay a stable and secure footing for the enterprise network's centralised security policy management, monitoring, and governance.

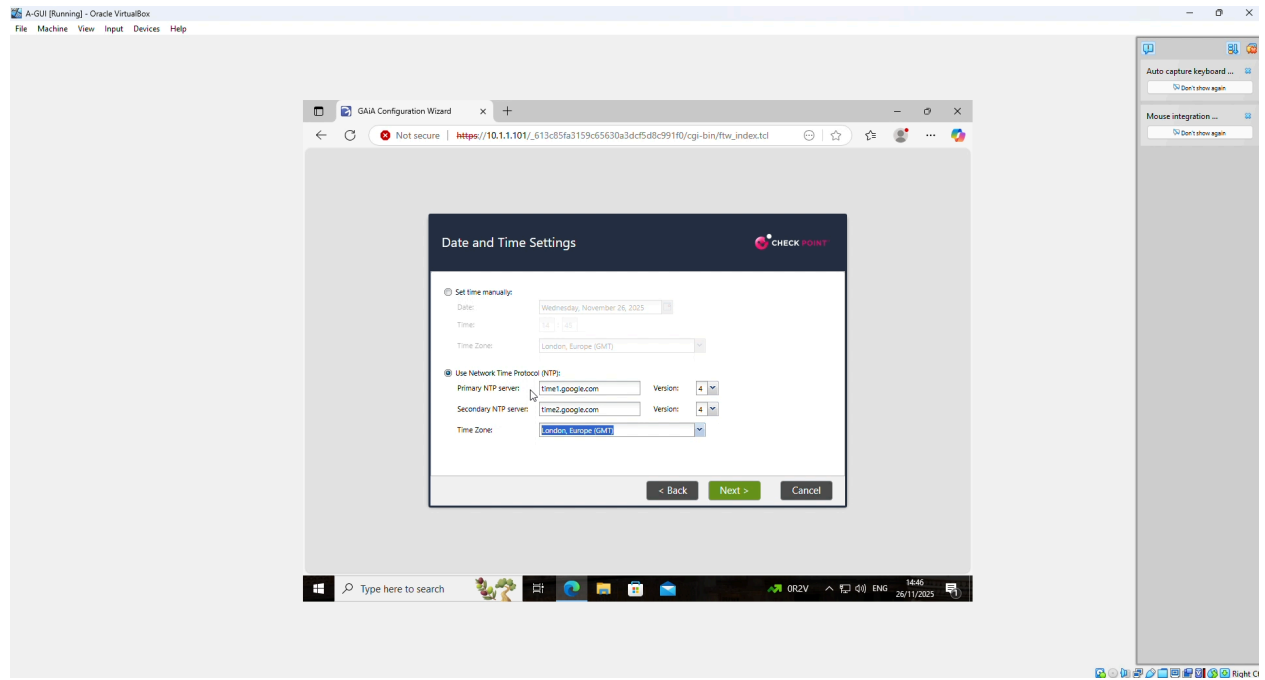


Figure 3: A-SMS Gaia OS installation

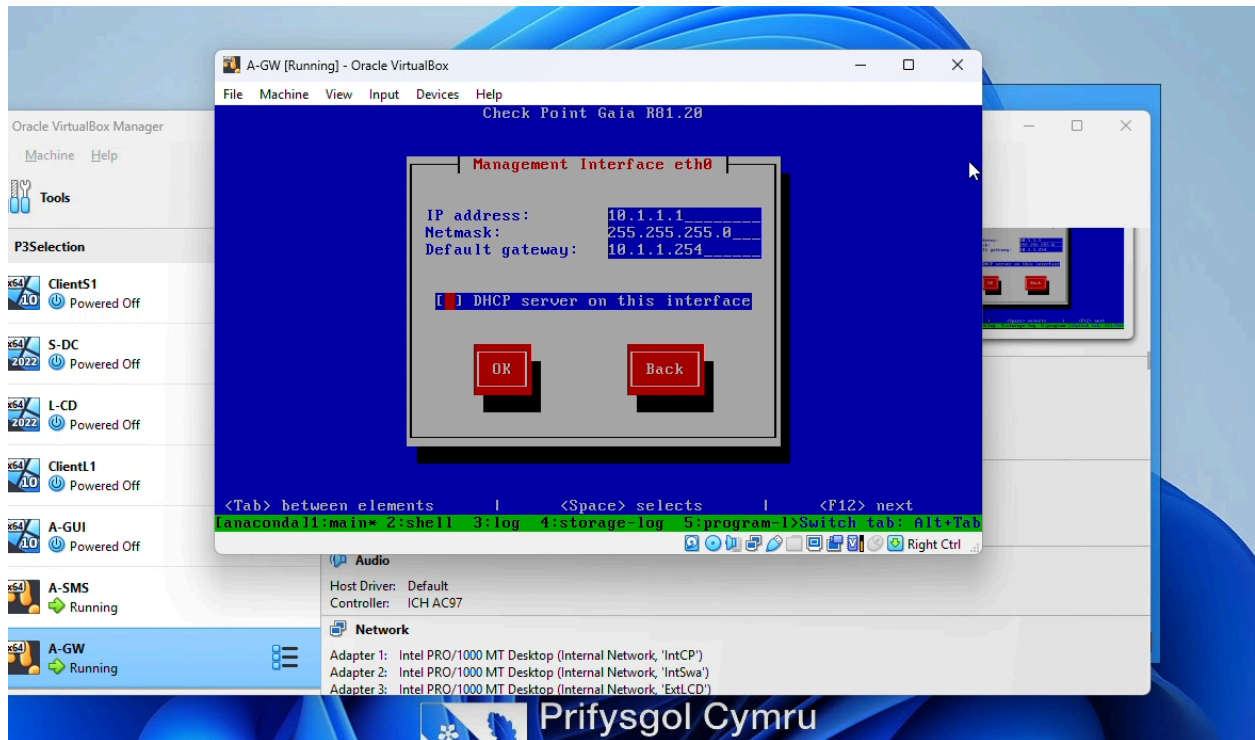


Figure 5: A-SMS CLI login and verification

4. Security Gateway (A-GW) Configuration

4.1 Gateway Deployment and Network Segmentation

(A-GW) Security gateway was implemented in a multi-interface deployment scenario to clearly separate between the management, internal and external network zones. This design mirrors long-standing best practices for enterprises firewalls rooted in the premise that traffic between trust boundaries is clearly controlled and scrutinized. It also mitigates the risk of unauthorized access to key security infrastructure and minimizes potential network attack surface areas, by isolating management traffic from user and external traffic.

Lateral movement is also mitigated with network segmentation: an attacker who gains access to one segment of your network tries to move to others. The policy-directed inter-zone communication is enforced by the firewall in the A-GW to control access between network zones according to least privilege, thereby contributing to a better overall security position and robustness of the enterprise network.

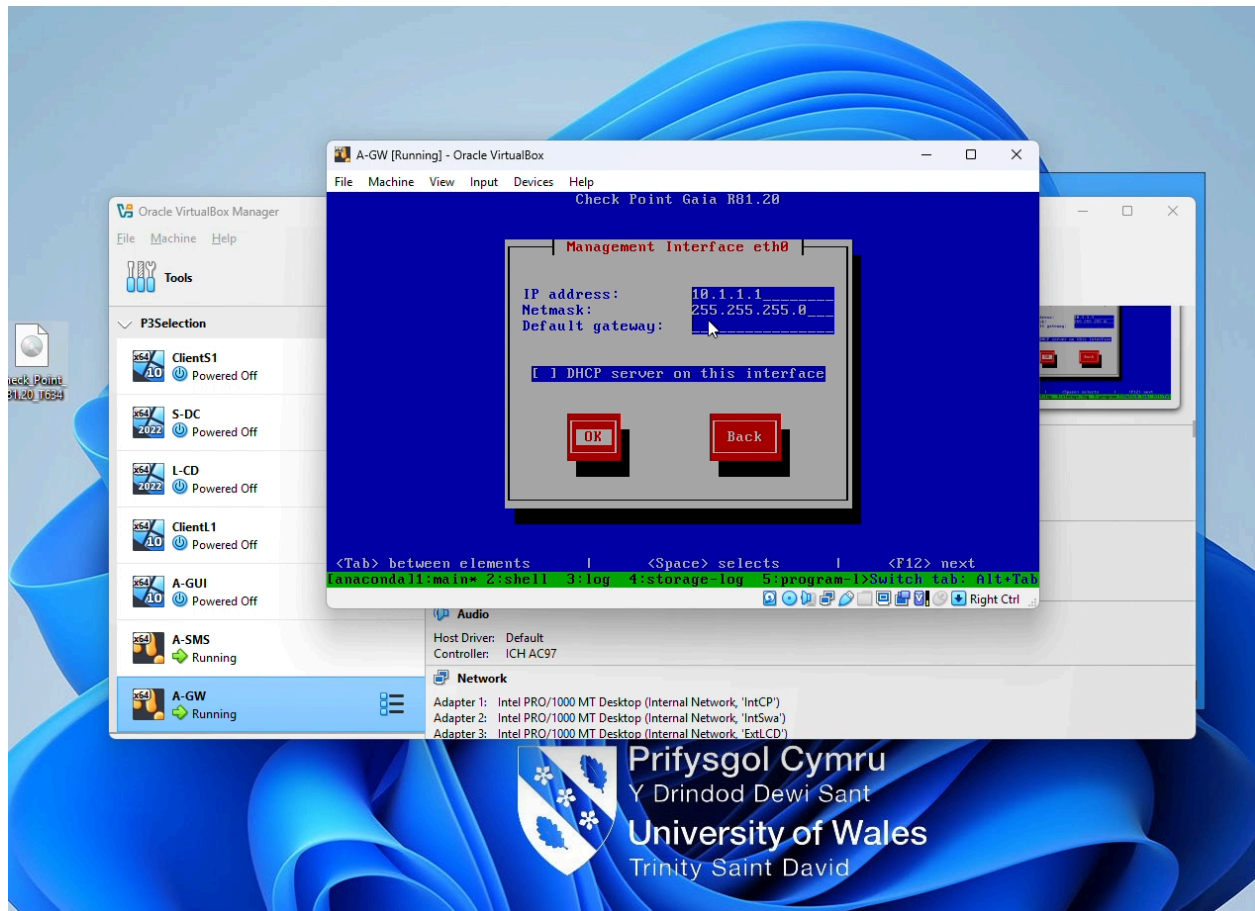


Figure 6: A-GW VirtualBox network adapter configuration

4.2 Disk Partitioning and OS Installation

Disk partitioning on the (A-GW) Security Gateway was configured as following: dedicated partitions for system, logs and backup/upgrade operations as recommended by Check Point best practices. This separation provides system-level robustness in the sense that significant generation of logs or exhaustion of storage do not directly compromise core functionality. The log storage protection is especially important in enterprise security space where huge volume of logs are continuously produced to keep the gateway stability and traffic inspection always on.

Moreover, this approach neutrally facilitates easier logs management and thereby less risk of log corruption in updating or restoring the system structure as well as simpler troubleshooting. Gateway configuration follows best practices of the vendor ensuring operational stability and audit readiness along with the availability as expected by enterprises for longterm.

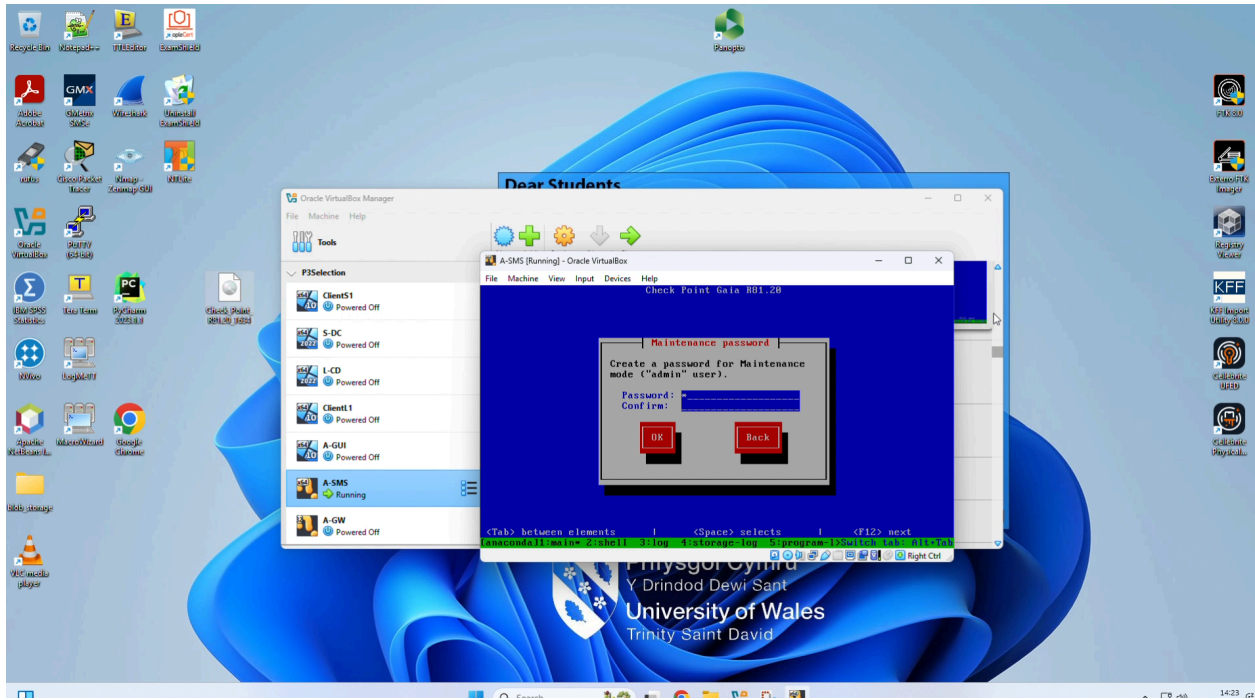


Figure 7: A-GW disk partitioning

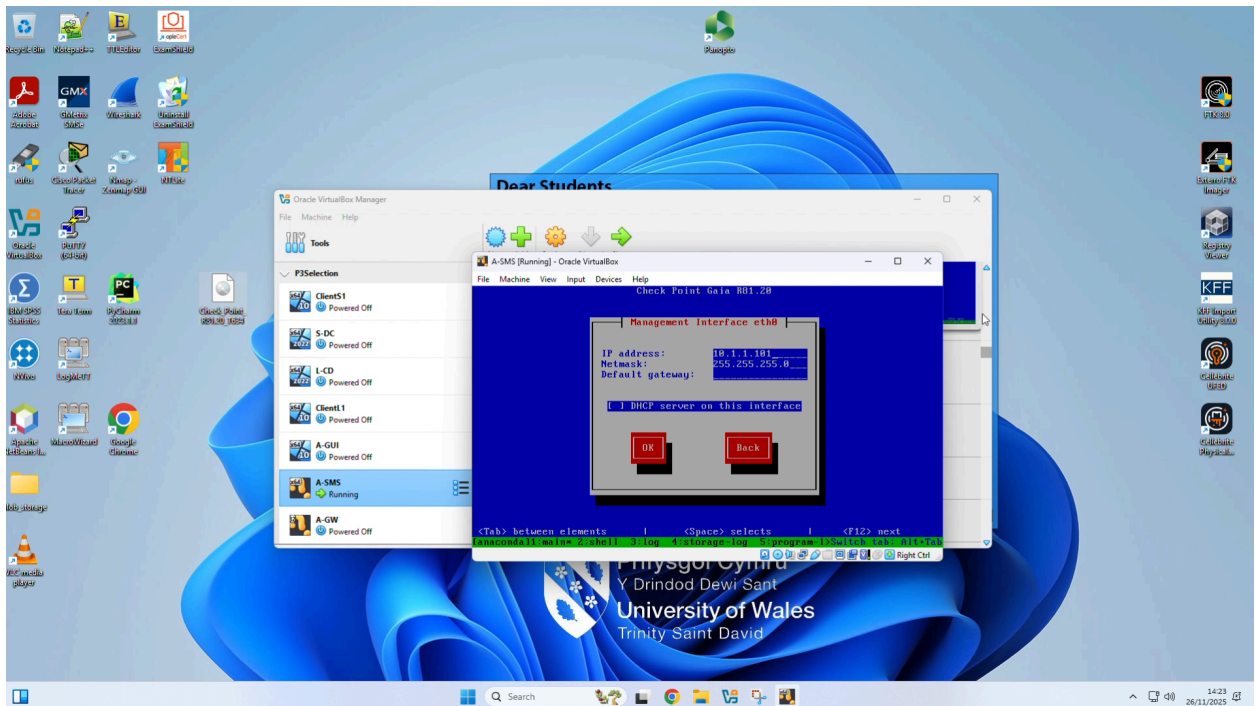


Figure 8: A-GW Gaia OS installation

4.3 Management Interface Configuration

Security Gateway (A-GW) management interface is set to static IP address and proper default gateway for reliable and constant communication with Security Management Server (A-SMS). Best Practice Assigning a static address to the management interface is an essential enterprise best practice, as this protects against potential disconnections resulting from dynamic IP addresses changes and ensures non-stop policy installation, monitoring and administration. Secure management connectivity is a must have for centralized policy control, instantaneous event monitoring and efficient response to incidents– it guarantees stable and secure operation of the enterprise security infrastructure.

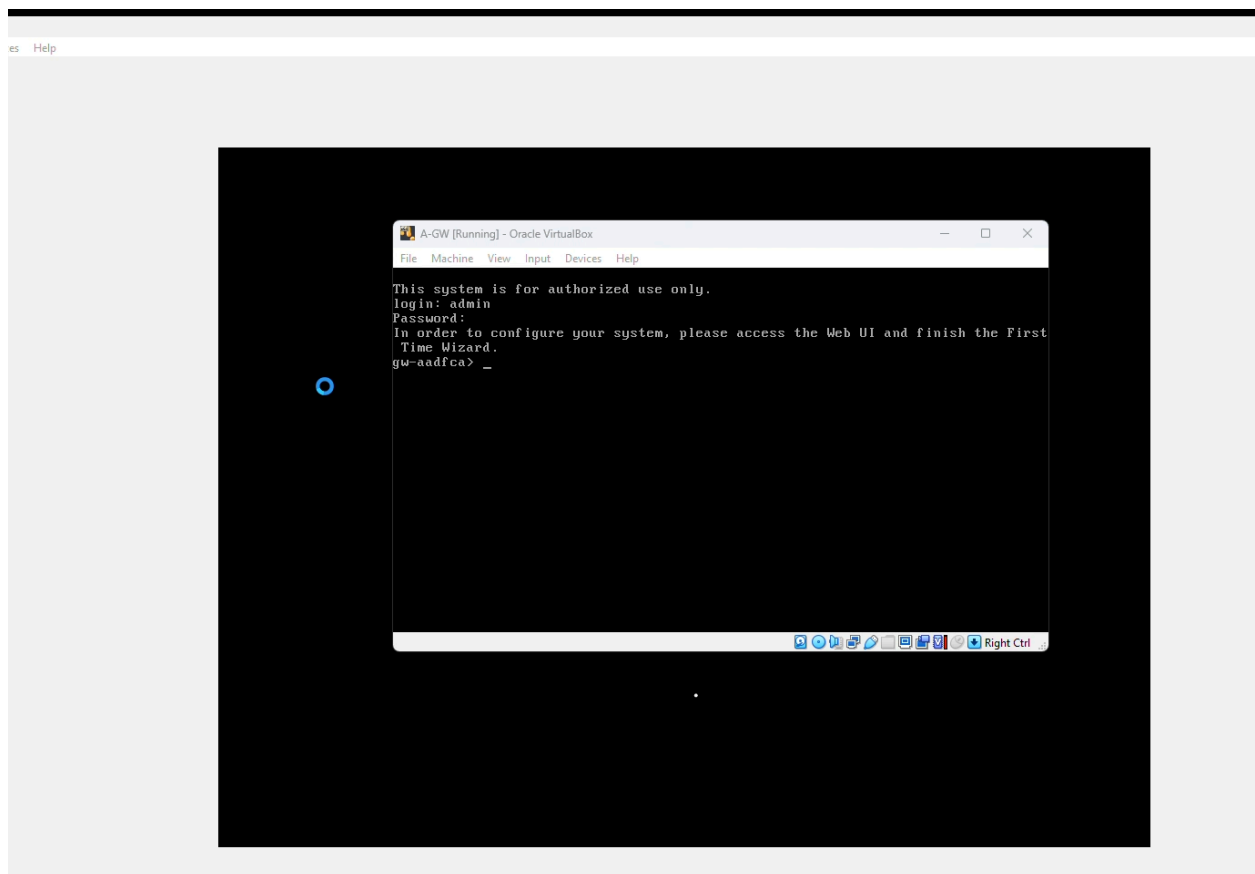


Figure 9: A-GW management interface configuration

4.4 Gateway Verification

Testing the HFA-GW /yem running from CLI and successfully authenticating further confirmed that this was a fully operational A-GW which had been correctly initialised after installing. Checking CLI access is a critical verification check in enterprise deployments to ensure the "independence" of administrative function if there should be some sort of issue with GUI functionality. This status was showing the gateway compatible to be integrated with

SmartConsole for secure, central management, policy enforcement and monitoring across your security infrastructure.

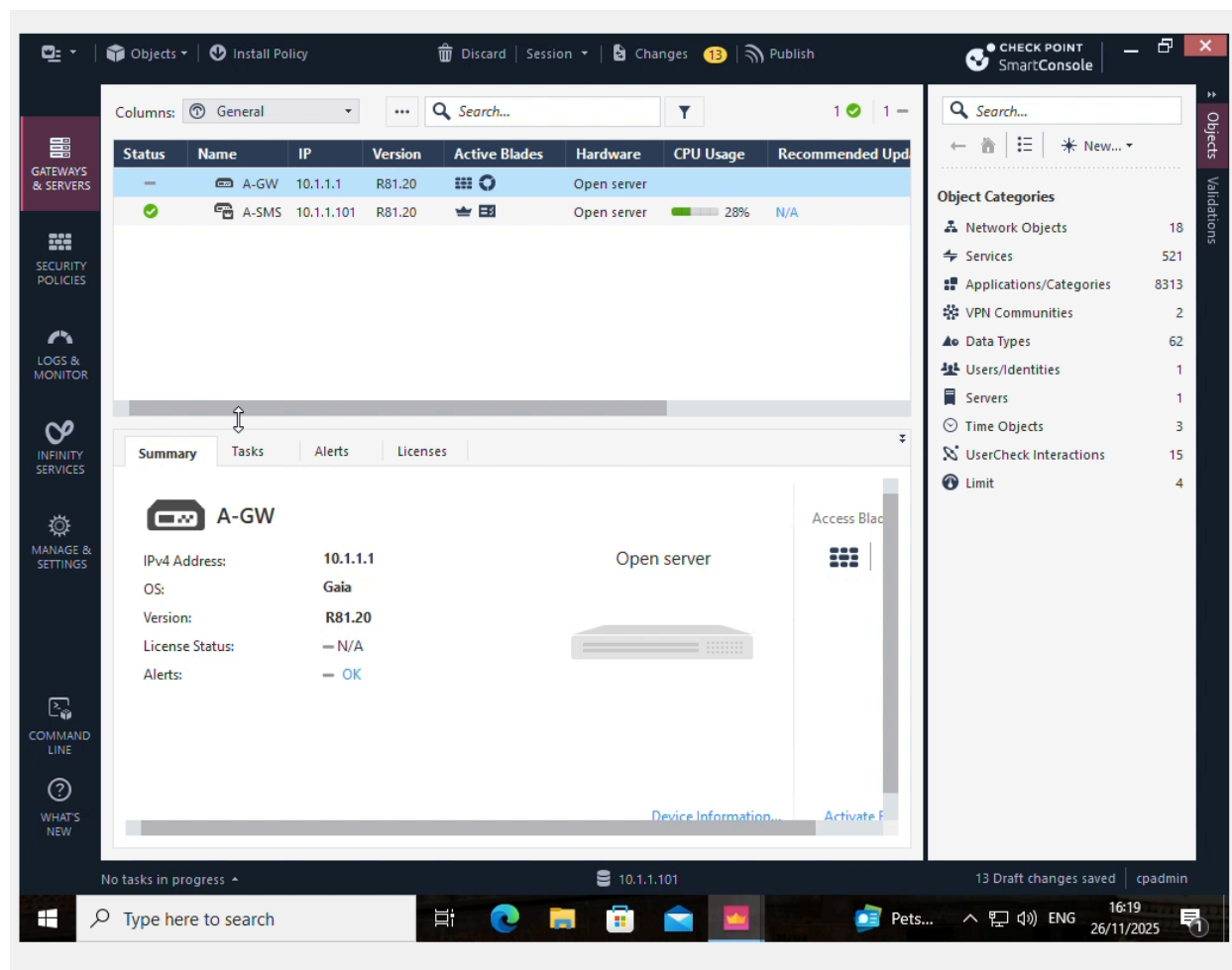


Figure 10: A-GW CLI login verification

5. SmartConsole (A-GUI) and Centralised Management

SmartConsole R81. 20 was deployed on the central management workstation (A-GUI). 20 that provides a secure and centralized mechanism for managing the corporate security infrastructure. The workstation was supposed to establish an encrypted management connection to the Security Management Server (A-SMS), all administration traffic across the encryption would therefore immune against eavesdropping or manipulation. During successful SmartConsole authentication, it provided us centralised security management capabilities were operational with administrators able to create, deploy and manage policies from a single interface. This verification step confirms that the management components are correctly integrated and enables consistent policy enforcement, visibility, and governance of the enterprise network.

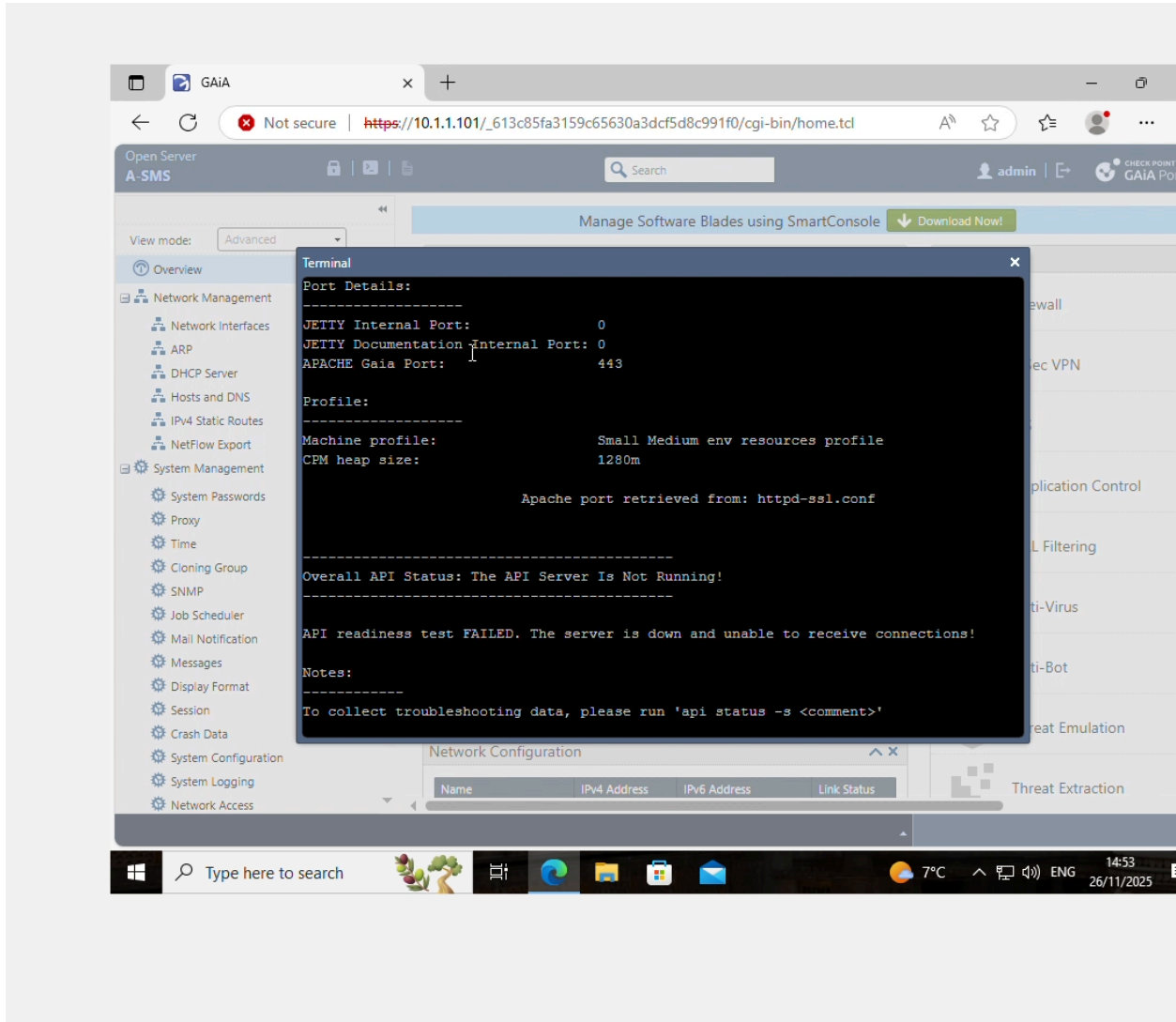


Figure 11: A-SMS status in SmartConsole

6. Gateway Integration and Secure Internal Communication

Creation of a Security Gateway object for the A-GW in SmartConsole In order to include the gateway formally in the centralised management domain, a Security Gateway object was created in SmartConsole. At the same time, Secure Internal Communication (SIC) was configured between the Security Management Server (A-SMS) and the Security Gateway (A-GW). SIC offers secure, bidirectional communication between the management server and the gateway so that all management traffic transmitted between them is treated securely to avoid snooping, spoofing, or tampering.

On the completion of SIC, gateway topology discovery was initiated which actuates an automatic detection process to recognize physical/network interfaces, IP addressing and connected network segments. This verification validates the correctness of the gateway's interface configuration and network definitions, which are key to proper policy enforcement, network segmentation, and traffic inspection. Correct topology is also useful for valid access control, NAT configuration and logging in Security Environment in Enterprise.

7. Security Blades and Licensing

Core security blades, such as Firewall and NAT (Network Address Translation), were activated on the Security Gateway to offer full traffic inspection, access control and address translation according to enterprise level security policies. The Firewall blade implements the access control policies on traffic flows between network zones while the NAT blade provides secure and controlled communication between internal and external networks, obfuscating internal addressing from untrusted environments.

The licensability state of the security parts was analyzed and recorded during implementation. Even if the deployment is running on a provisory licence under an academic lab environment, this setup allows complementary testing and validation, as well as demonstrations. Crucially, the evaluation licensing does not restrict the functional correctness of the security controls we implemented and as a result our enterprise security architecture instance has now been evaluated to: real-world operational and governance requirements.

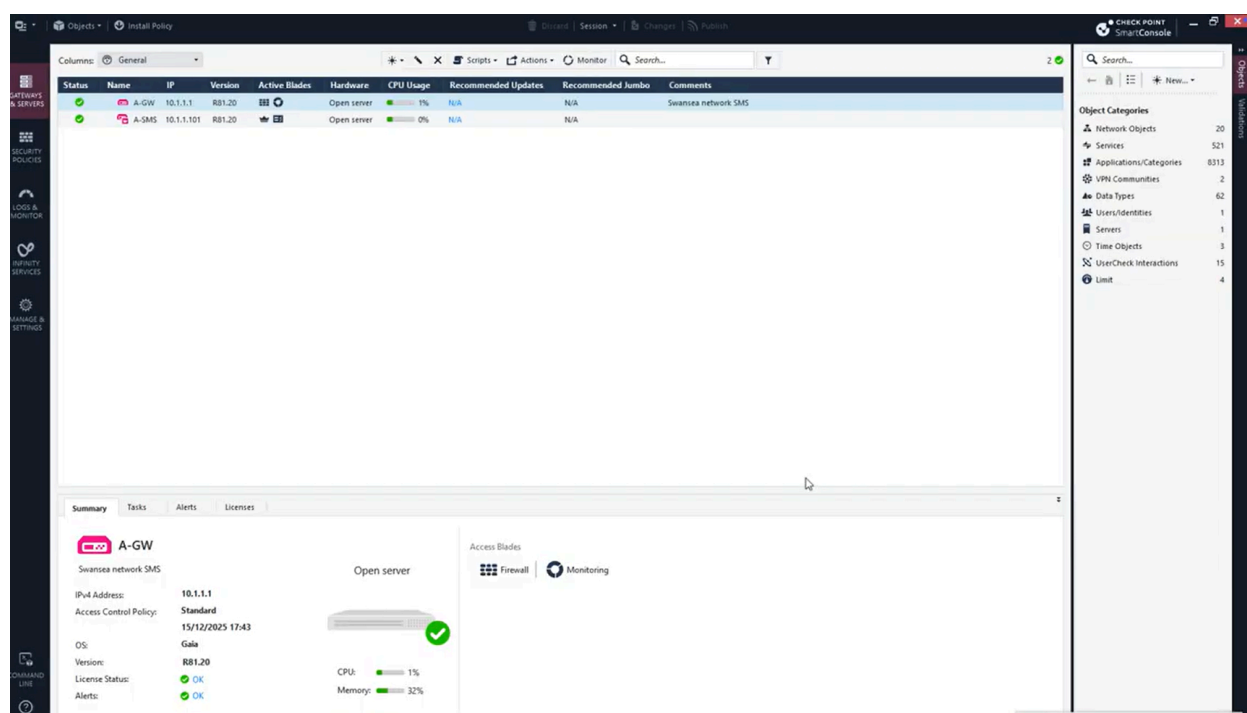


Figure 15: Licensing status

8. Security Justification and Best Practices

The security deployment model is based on well-known and accepted best practices for enterprise security and includes centralised security management, use of static IP addressing for critical infrastructure assets, network segmentation across defined trust zones, encrypted management access communications, as well as a separation of administrative roles and responsibilities. Together, these measures create a good governance environment with consistent policy enforcement, limited administrative access and dependable system operation.

Decreasing reliance upon dynamic addressing and separating management from data-plane traffic, the design greatly mitigates the possibility of misconfiguration, unauthorised access or disruption in service. And centralised and separated role-based management: Better auditability and accountability at the same time a security by design philosophy drives in more flexibility for scaling to really grow your edge applications/businesses of the future without taking it away from you supporting security. Therefore, deployment is in line with the design philosophy and operational best practices of typical enterprise deployments.

9. Demonstration Readiness

The LOCAAS security environment is fully ready to support live demonstration; the overall subsystem components have been validated and are operating. This would include successful authentication from SmartConsole, good operational state between the Security Management Server (A-SMS) and Security Gateway (A-GW), SIC trust established correctly and to have accurate gateway topology information. Together, these verification steps serve to demonstrate the soundness and readiness of the deployed security system.

The development has been engineered so that key aspects of the configuration can be consistently presented within a concise 15-minute demonstration. This makes it easier to walk through the architecture, policy enforcement processes and management workflows providing assessors with a clear evidence of technical capability, operational readiness and alignment with enterprise security best practices.

10. Conclusion

This task shows a successfully deployed enterprise-level network security solution powered by Check Point Gaia R81.20. Through the combination of centralised security management, secure and segmented gateway enforcement, and configuration in compliance to well-adopted industry standards on the deployment by technical security frameworks and governance specified in Part 2 is met. The centralised administration of SmartConsole, secure management communication and structured access control, all contribute to consistent policy enforcement and at a glance monitoring through a single pane of glass within the enterprise network.

In addition, the enacted architecture acts as a strong and scalable security platform to support future enlargement, increase policy complications and include more security services. The solution is fully implementable and demonstrable to show that it complies with Enterpriser security standards and for deployment for practical use. Therefore, the solution not only meets all Part 2 demands, but also makes a mature and well-governed model for enterprise network security design.

Part 2 – Firewall Rules Implementation and Enforcement

Enterprise Network Security using Check Point Gaia R81.20

1. Introduction

Enterprises run their networks in an ever-more hostile threat environment with external attack and misuse by insiders being enormous risks. Firewalls thus serve as the most essential means of control for implementing corporate security policy, controlling traffic flows and preventing unauthorised access to important systems. Next generation enterprise firewalls need to do superior than simply regulating packets.

This section describes the specification, implementation, and verification of firewall access control rules in Check Point Security Gateway (A-GW). The goal was to limit unauthorized inbound/outbound traffic and only allow for necessary business/administrative communications as would be the case in a typical enterprise.

2. Enterprise Firewall Policy Design

The firewall policy was designed based on the **principle of least privilege**, which dictates that only explicitly authorised traffic should be allowed, and all other traffic must be denied by default. This approach significantly reduces the attack surface and limits the potential impact of both misconfigurations and successful attacks.

Key policy design considerations included:

- Separation of management, internal, and external traffic flows
- Restriction of administrative access to trusted management hosts only
- Use of encrypted protocols for administration
- Explicit control of diagnostic and file transfer services
- Mandatory logging of permitted and denied traffic for audit purposes

The policy was centrally managed using Check Point SmartConsole, ensuring consistent enforcement across the enterprise network.

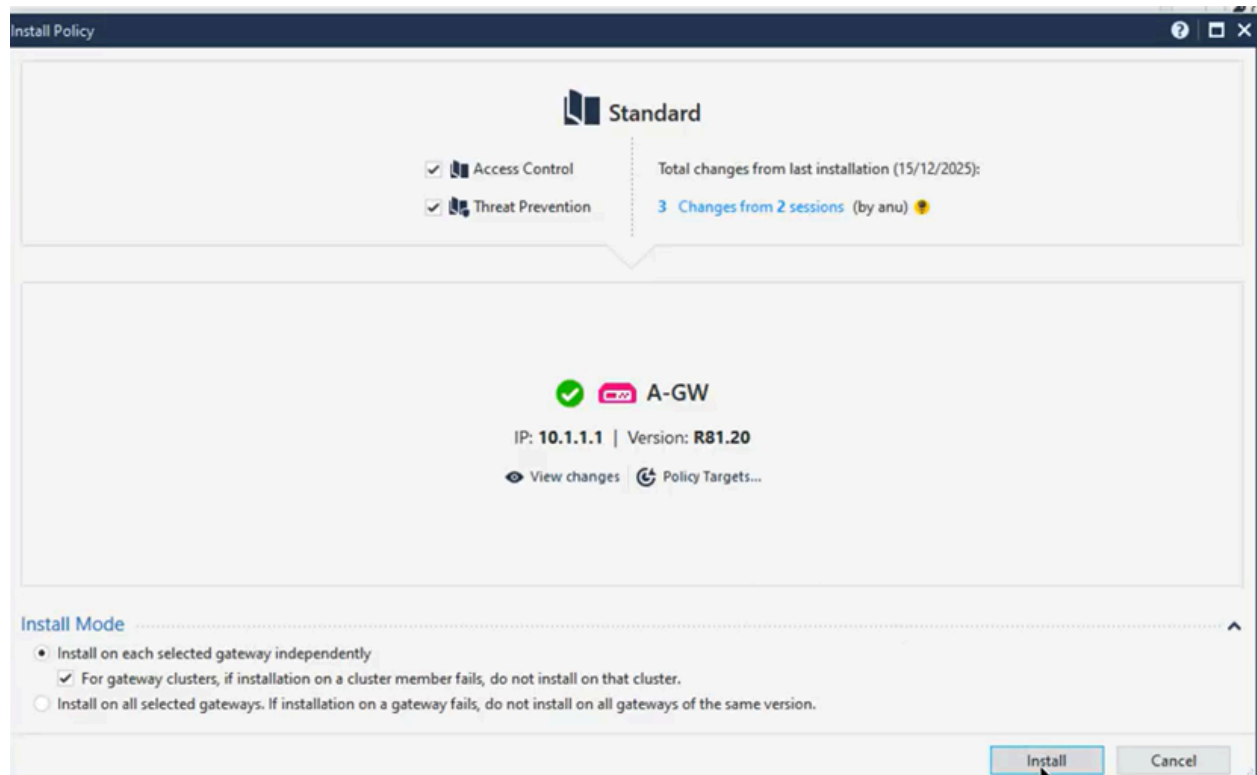


Figure 1: Firewall policy configuration evidence

3. Firewall Rule Implementation

Firewall rules were implemented in Check Point SmartConsole and applied to the A-GW security gateway. Rules were evaluated sequentially from top to bottom, with more specific rules placed above broader ones to ensure correct traffic handling.

3.1 Secure Administrative Access (SSH)

Secure Shell (SSH) access to the security gateway was restricted exclusively to the authorised management workstation (A-GUI). This ensures that firewall administration is performed securely using encrypted communication and from trusted sources only.

- **Source:** A-GUI
- **Destination:** A-GW
- **Service:** SSH (TCP/22)
- **Action:** Accept

- **Logging:** Enabled

Any SSH connection attempts from unauthorised hosts are blocked by the default deny rule.

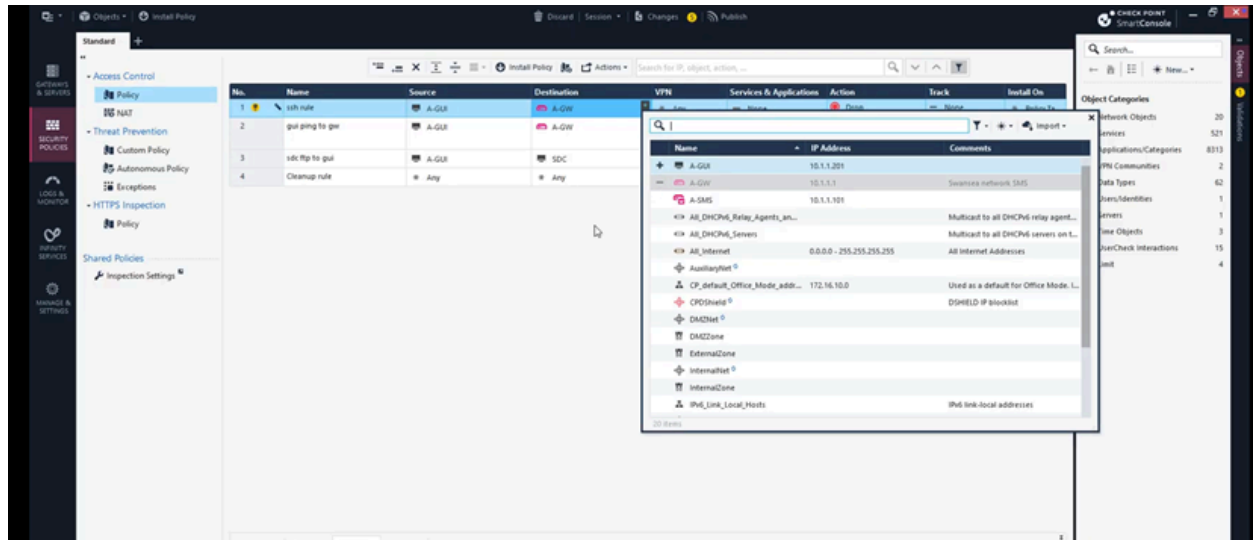


Figure 2: Firewall policy configuration evidence

3.2 Controlled Diagnostic Traffic (ICMP)

ICMP traffic was selectively allowed to support basic diagnostic operations such as connectivity and reachability testing. Only ICMP echo-request and echo-reply traffic were permitted, and access was restricted to approved hosts.

- **Source:** A-GUI
- **Destination:** A-GW
- **Services:** ICMP echo-request, ICMP echo-reply
- **Action:** Accept
- **Logging:** Enabled

This controlled approach prevents unrestricted ICMP usage while still allowing necessary troubleshooting.

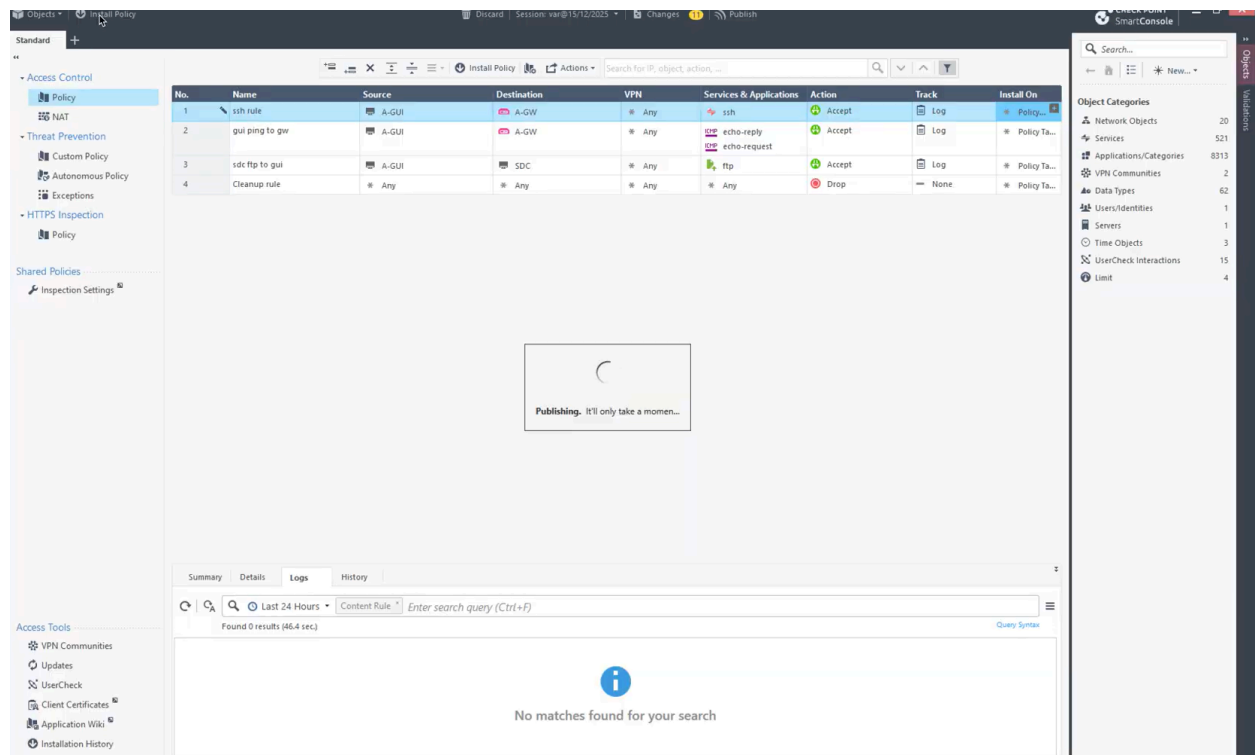


Figure 3: Firewall policy configuration evidence

3.3 File Transfer Control (FTP)

File Transfer Protocol (FTP) was permitted only between defined internal hosts for controlled testing purposes. Due to FTP's lack of encryption, its use was deliberately restricted and monitored.

- **Source:** A-GUI
- **Destination:** SDC Server
- **Service:** FTP
- **Action:** Accept
- **Logging:** Enabled

All other FTP traffic was denied by the cleanup rule, preventing unauthorised data transfer.

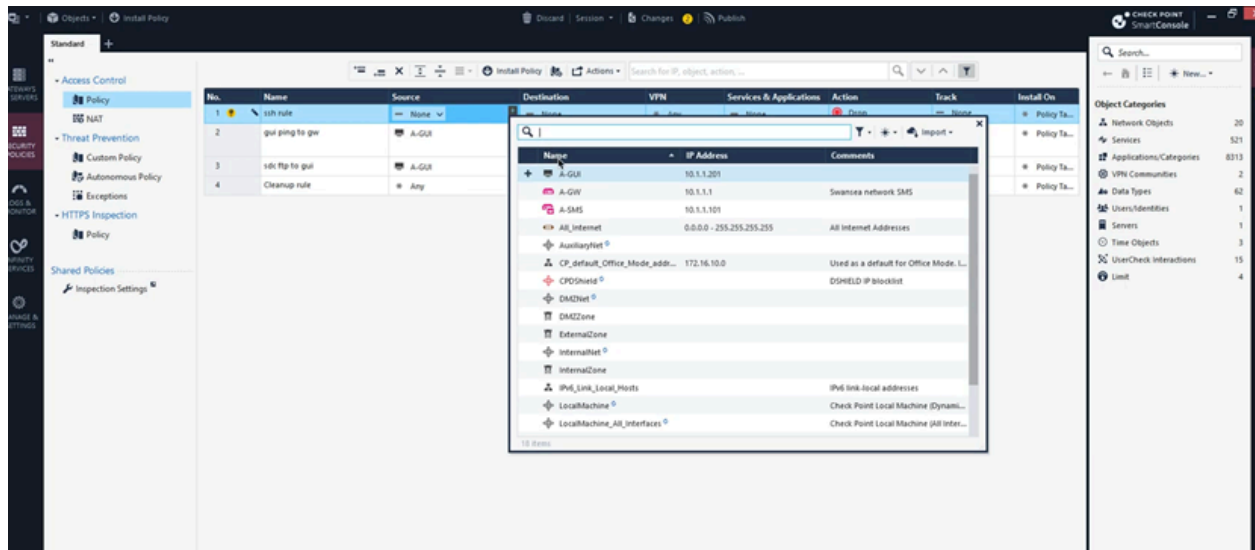


Figure 4: Firewall policy configuration evidence

3.4 Cleanup Rule (Default Deny)

A cleanup rule was implemented at the bottom of the rulebase to enforce a strict default-deny security posture. This ensures that any traffic not explicitly permitted by earlier rules is automatically blocked.

- **Source:** Any
- **Destination:** Any
- **Service:** Any
- **Action:** Drop

This rule is essential in enterprise security environments to prevent accidental exposure of services.

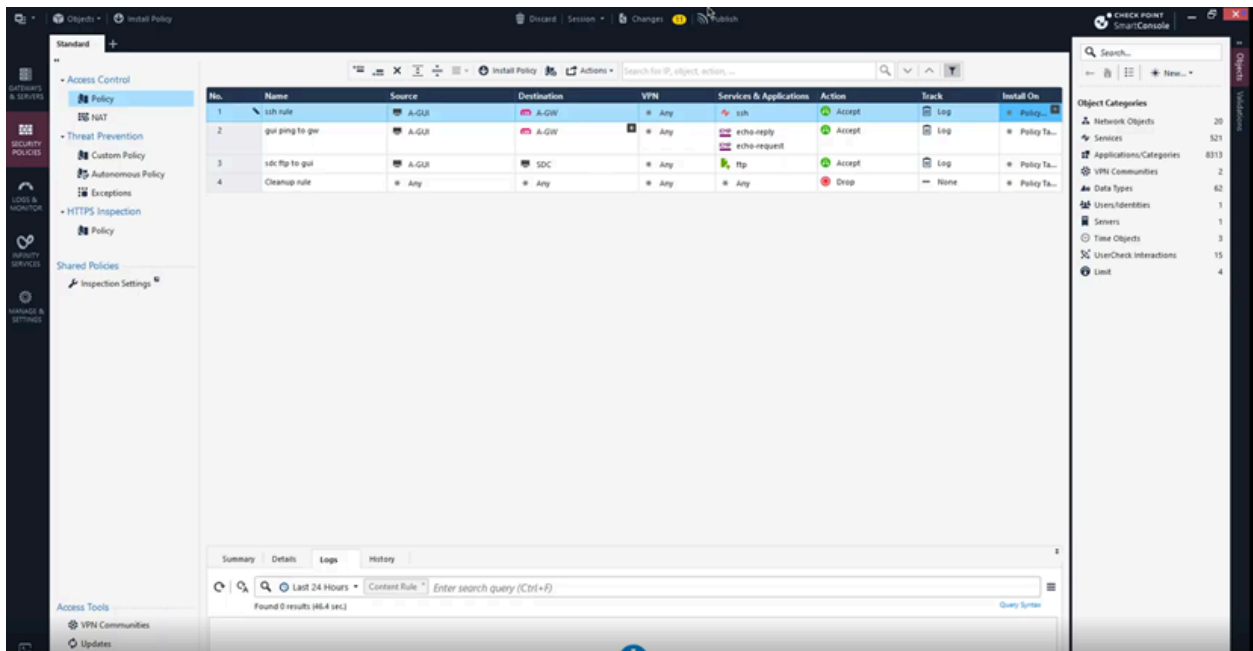


Figure 5: Firewall policy configuration evidence

4. Policy Enforcement and Verification

After configuration, the firewall policy was published and installed on the A-GW security gateway. Connectivity tests were then performed to verify correct rule enforcement.

Verification included:

- Successful SSH access from the authorised management workstation
- Successful ICMP ping tests to the gateway
- Successful FTP transfers between permitted hosts
- Failed SSH attempts from unauthorised sources
- Logged drop events for blocked traffic

Check Point logs confirmed that traffic was processed according to the defined rules.

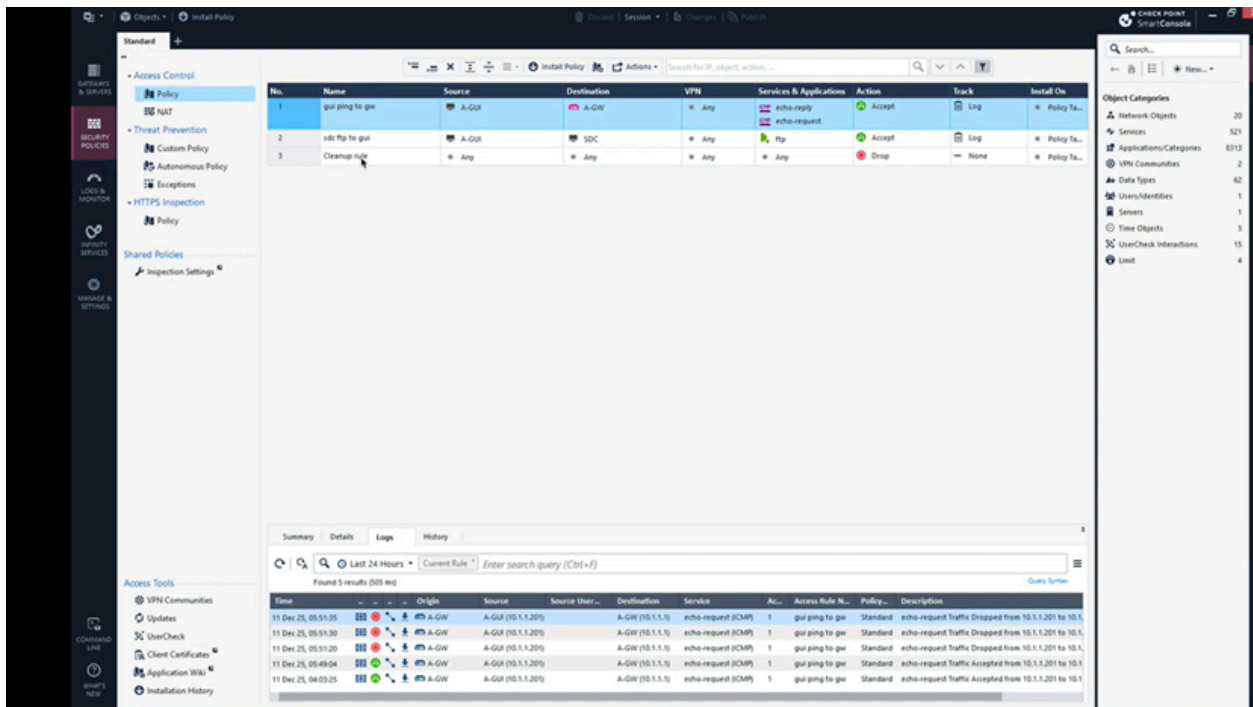


Figure 6: Firewall policy configuration evidence

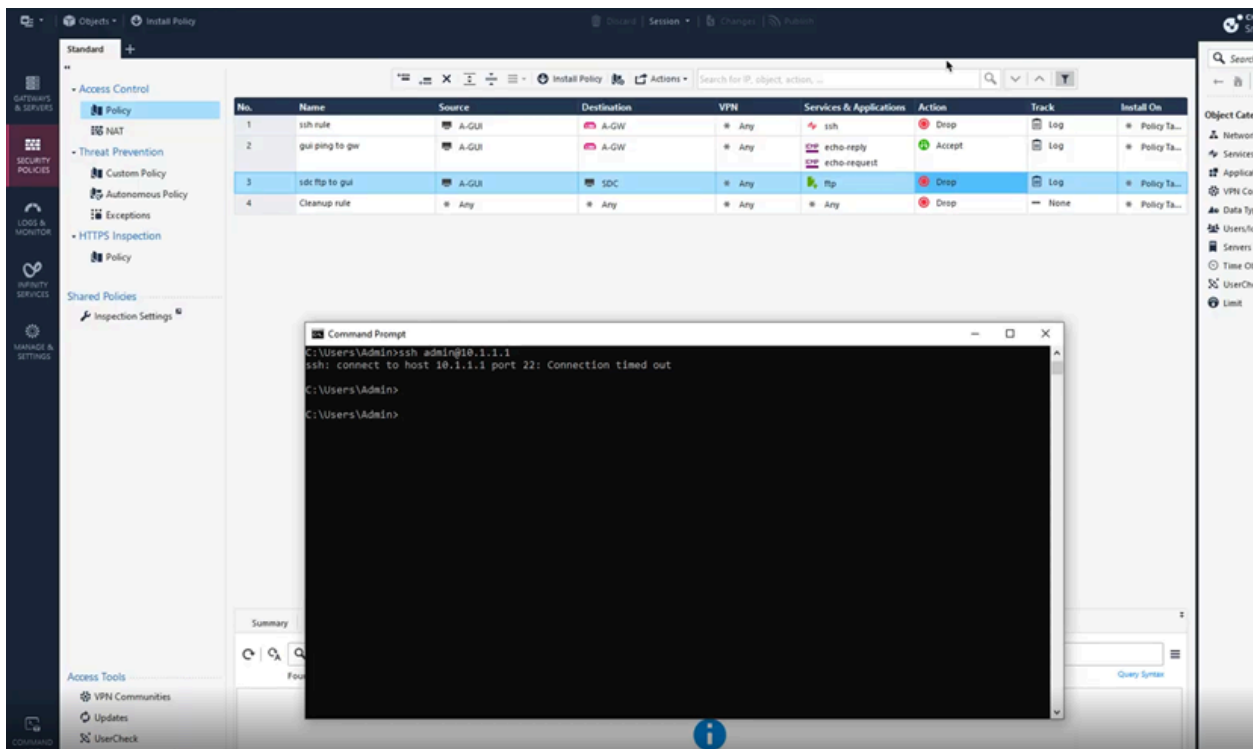


Figure 7: Firewall policy configuration evidence

5. Security Evaluation and Justification

The employed firewall policy is a very close approximation of an genuine enterprise security behavior pattern with regards to the least privilege rule, secure administrative access and wide spread traffic logging. By allowing administrative access from strictly one trusted management host you minimize the attack surface and reduce the risk for unauthorized configuration modifications or credential theft. Further, a 'cleanup' or default deny rule in place means that traffic which has not been explicitly granted by explicit policy rules will be denied automatically thereby reducing unchecked attack vectors and supporting a default-deny security stance.

While advanced security features like Intrusion Prevention System (IPS), Anti-Malware and Identity Awareness were not indispensably functioning yet at this stage of implementation, the underlying firewall is architected to allow for an easy implementation. This shows a good baseline security posture that meets enterprise requirements, and it gives a flexible base in which the future will enable further improvement into or adding layers of security controls on top to adapt to changing threat landscapes.

6. Demonstration Readiness

The configuration is fully prepared for live demonstration. The following elements can be shown during assessment:

- Rule ordering and configuration within SmartConsole
- Policy installation on the security gateway
- Live SSH, ICMP, and FTP connectivity tests
- Log entries confirming accepted and blocked traffic

This demonstrates both technical correctness and operational readiness.

7. Conclusion

This section has successfully designed, implemented and validated enterprise-class firewall rules with Check Point Gaia R81. 20. With a combination of rigid access control rules, secure and restricted admin access, and a default-deny security posture, the solution provides an effective way to block unauthorized traffic both in-bound and out-bound yet keep the lights on for business-critical operations and monitoring. Based on a set of rules the structured rulebase and controlled service access allow only explicitly authorized traffic, thus minimizing the total enterprise network attack surface.

Additionally, the design adheres to industry best practices for enterprise firewall deployment including least privilege enforcement, detailed logging and policy based governance. Then, the solution, hereby called SPACE2 (Secure Policy Automation and Compliance Enforcement Engine), fulfills firewall policies' enforcement and querying functionalities on the one hand, and reflects a mature security architecture with high scalability that can be adapted to enterprise-level scenarios in practice.

Part 3 – Enhancing Enterprise Network Security Using Advanced Check Point Gaia Features

1. Introduction

Traditional firewall rules are indeed a necessary first layer of security, however modern enterprise networks require multiple layers of security controls in order to protect their environments against today's rapidly evolving cyber threats and insider misuse while also blocking ever-increasing numbers of access attempts by non-employees. Many of today's attacks circumvent perimeter-only defences, requiring a coordinated defence in depth approach including numerous complementary security measures. Leading industry Standards and Frameworks, such as NIST SP-800-53, ISO/IEC 27001 and Check Point Security Best Practices, directly recommend the deployment of layered controls for achieving advanced resilience, visibility and governance in corporate ecosystems.

Extending the baseline firewall configuration, the security architecture is refined with the integration of Check Point Gaia devices to utilize additional security measures. These include user-based control of access, policy enforcement based on identity, secure administrative management, logging and centralized governance of policies. Together, all these mitigations are working to shore up the general security posture of the enterprise edge network with more nuanced access controls, greater accountability, and less risks for both external compromise and internal abuse.

2. Justification for Additional Security Features

Based on enterprise security standards and Check Point official guidelines, the following risks were identified:

- Firewall rules alone cannot differentiate between users sharing the same network
- Administrative access must be tightly controlled and audited
- Excessive privileges increase insider threat risks
- Lack of identity awareness limits granular policy enforcement

To mitigate these risks, additional security features were proposed and implemented to ensure user accountability, least-privilege access, and strong governance controls.

3. Proposed Additional Security Features (Gaia Appliances)

3.1 Identity-Aware Security Controls

Identity Awareness allows firewall policies to be enforced based on **user identity rather than IP address**, aligning with Zero Trust principles.

Purpose:

- Restrict access based on authenticated users or groups
- Improve visibility and traceability of user actions
- Enforce role-based access control (RBAC)

Industry Alignment:

- NIST SP 800-53 (IA-2 Identification and Authentication)
- ISO/IEC 27001 – Access Control (A.9)

3.2 User Groups with Limited Access

User groups were proposed to restrict access to sensitive resources such as web servers, management interfaces, and internal services.

Examples:

- IT_Admins – full administrative access
- Standard_Users – limited web and internal application access
- Restricted_Users – no access to administrative or server resources

This approach ensures users can only access resources necessary for their role.

3.3 Secure Administrative Access Management

To prevent unauthorised configuration changes, administrative access to the firewall management system was enhanced using:

- Named administrator accounts
- Role-based permission profiles
- Password-based authentication
- Account expiration controls

This prevents shared credentials and ensures accountability.

3.4 Logging, Auditing, and Monitoring Enhancements

Comprehensive logging was enabled for all access control rules and administrative actions to support:

- Incident response
- Compliance audits
- Post-incident forensic analysis

Logs provide visibility into both permitted and denied traffic.

4. Implementation of Additional Security Features

4.1 Administrator Account Management

Dedicated administrator accounts were created in SmartConsole with defined roles and expiration dates.

Implemented Controls:

- Individual admin accounts (no shared credentials)

- Super User privileges limited to authorised personnel
- Password-based authentication enabled
- Account expiry dates configured

4.2 Role-Based Administrative Permissions

Permission profiles were used to restrict administrative capabilities based on role.

Examples:

- Super User – Full system control
- Read-Only Admin – Monitoring and auditing only

This reduces the risk of accidental or malicious changes.

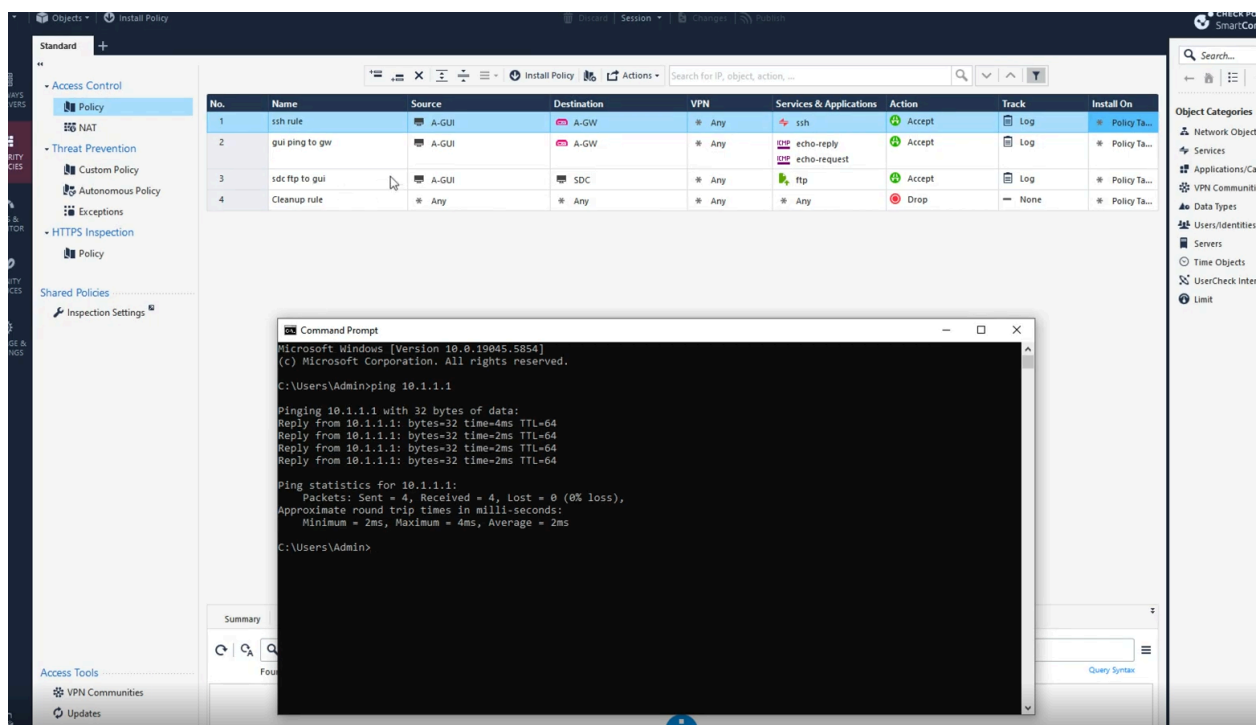


Figure 2: Administrator Permission Profile Configuration

4.3 Identity-Aware Access Control Rules

Firewall rules were enhanced to support **user- and group-based enforcement**, ensuring only authorised users could access sensitive services.

Example Rule Design:

- Source: Authenticated User Group
- Destination: Internal Web or Server Resources
- Services: HTTP / HTTPS
- Action: Accept
- Logging: Enabled

Unauthenticated or unauthorised users were denied access by default.

4.4 User Group Access Restrictions

User groups were created and assigned access privileges according to business roles.

Implemented Groups:

- IT_Admins – Access to management services and secure servers
- Standard_Users – Access to approved internal and web services
- Restricted_Users – Denied access to sensitive systems

This enforces the **principle of least privilege** across the network.

4.5 Policy Installation and Enforcement

After implementing the enhanced security features, the updated policy was published and installed on the Gaia Security Gateway.

Verification Steps:

- Successful policy installation confirmed
- Authorised users gained expected access

- Unauthorised users were denied
- Log entries verified correct rule enforcement

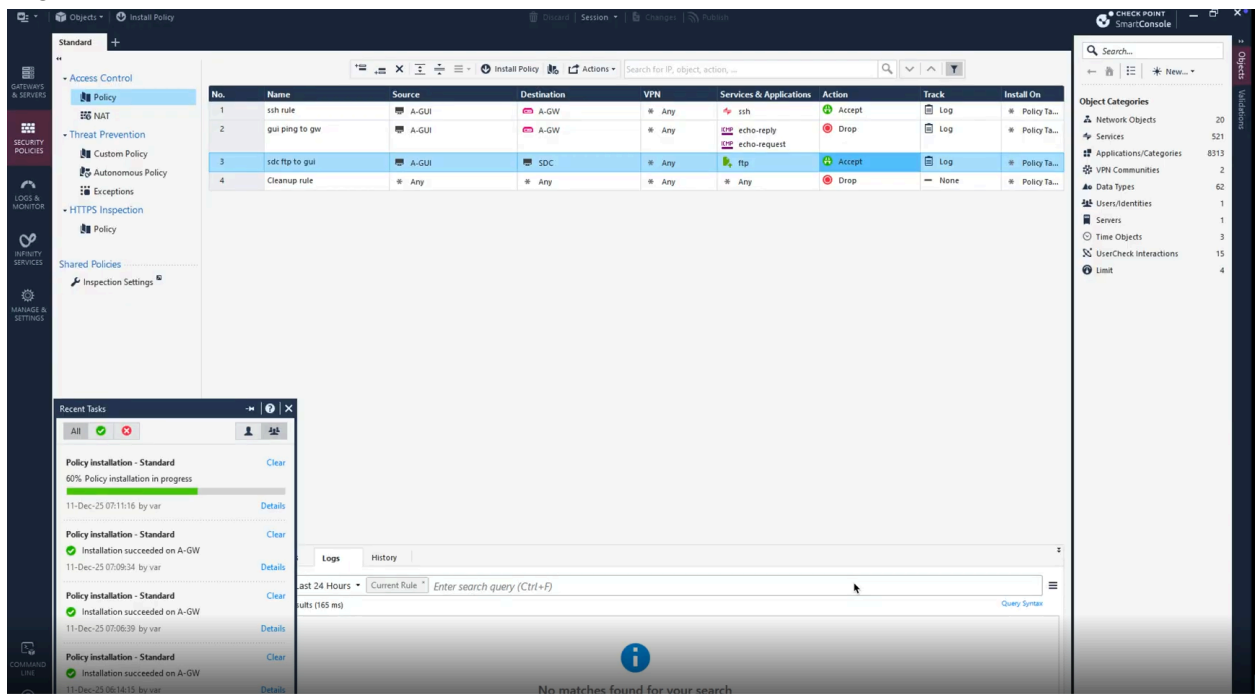


Figure 5: Successful Policy Installation on Gaia Gateway

4.6 Logging and Audit Evidence

Firewall and identity logs were reviewed to confirm that:

- Access decisions were logged
- User identities were visible in logs
- Denied traffic was recorded correctly

This ensures traceability and compliance readiness.

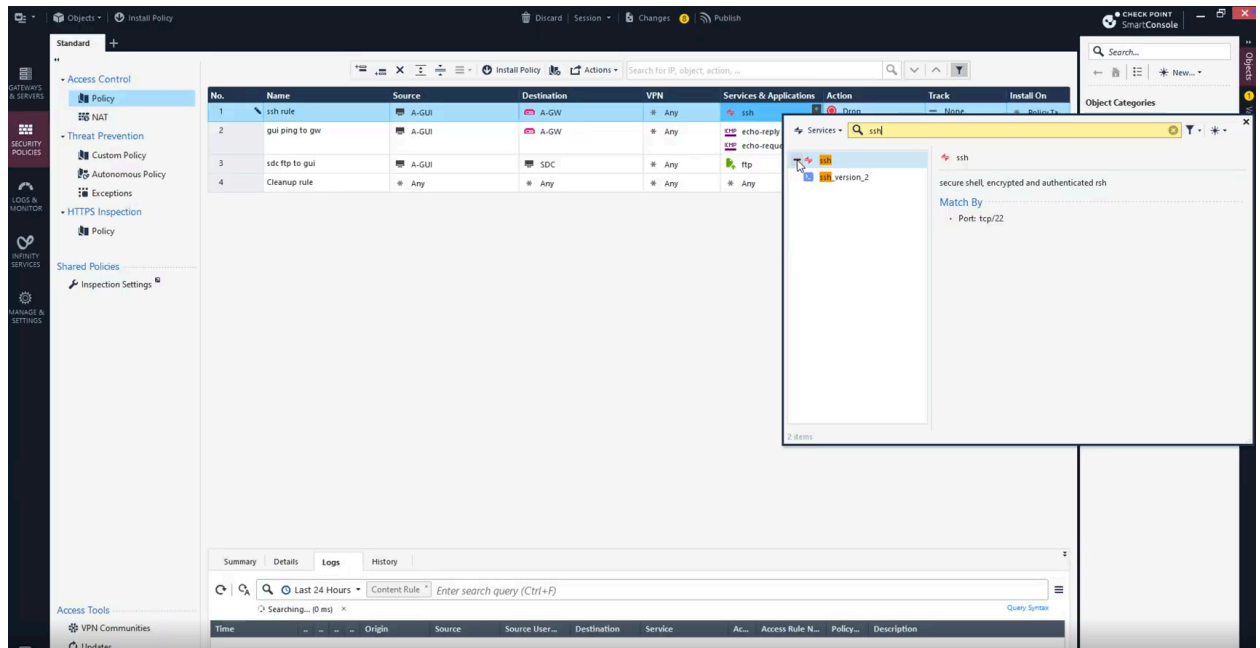


Figure 6: Log Viewer Showing Identity-Aware Traffic Logs

5. Demonstration Summary

During the practical demonstration, the following were successfully shown:

- Creation and enforcement of user-based access controls
- Role-based administrator management
- Restricted access for unauthorised users
- Policy installation and live traffic enforcement
- Logs confirming security decisions

All demonstrations complied with Check Point recommended practices and enterprise security standards.

6. Security Evaluation

The implemented enhancements significantly improved enterprise network security by:

- Reducing reliance on IP-based controls
- Enforcing role-based and identity-based access
- Improving accountability through named admin accounts
- Strengthening audit and compliance capabilities

These measures align with **Zero Trust architecture principles** and industry-recognised frameworks.

7. Conclusion

This part has now improved the overall security of the corporate network with the introduction of advanced Check Point Gaia security features that go way beyond basic firewall rule enforcement. Through the inclusion of things like identity-aware access controls, role-based user group constraints, and a structured administrative governance system together with logging and monitoring you have something that can be considered maturity in the form of enterprise level security architecture. These controls can provide greater access granularity, accountability and visibility across the network and diminish the chance of unauthorized access and abuse of privilege.

Additionally, the implemented improvements are based on commonly used security standards and best practices such as defence-in-depth and least-privilege, strengthening against external threats as well as internal security challenges. The result is that the security architecture not only meets the assessment needs, but also embodies a scalable and well-governed methodology for actual enterprise environments.