

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

Raju Molla

Programme: MSc in Cybersecurity and Digital Forensics

Module: Enterprise Network Security

Module code: ACCA7032

Table of Contents

1. Introduction
2. Purpose of Using A-SMS, A-GW, and A-GUI
 - 2.1 A-SMS (Security Management Server)
 - 2.2 A-GW (Security Gateway)
 - 2.3 A-GUI (Management Workstation)
3. Deployment Order and Methodology
4. A-SMS Configuration (Security Management Server)
5. Troubleshooting A-SMS Status Failure
6. SmartConsole Installation on A-GUI
7. A-GW Configuration (Security Gateway)
8. Verification of Connectivity (Swansea Network ↔ A-SMS)
9. Licensing Configuration and Verification
10. Enterprise Firewall Policy Design (Justification)
11. Firewall Rules Configuration
 - 11.1 SSH Access Rule (Remote Administration)
 - 11.2 ICMP (Ping) Rule – Connectivity Verification
 - 11.3 Cleanup Rule (Default Deny)
12. Policy Installation and Enforcement
13. Verification of Remote Access (SSH)
14. Administrator and User Access Control
 - 14.1 Creating New Administrator Accounts
 - 14.2 Logging in Using New Administrator
15. Security Benefits of Role-Based Administration
16. Additional Security Enhancements (Alignment with Standards)
17. Conclusion

1. Introduction

This study shows how to design, set up, and test a secure enterprise network using Check Point Gaia appliances and security best practices that are widely accepted in the industry. The main goal was to create a centrally managed security architecture with strong access control, centralized administrative management, and enforced network security policies.

To do this, they built a centralized management system using a Security Management Server, a Security Gateway, and a management workstation running SmartConsole. This design makes operations more efficient, scalable, and secure by separating management, enforcement, and administrative tasks. Centralized policy control makes it possible for the whole company network to have consistent security enforcement, easier monitoring, and faster audits.

Along with setting up the infrastructure, firewall access control policies were made using the least privilege idea. This means that only the services that are needed are allowed, and all other traffic is blocked. Role-based management and secure administrative access were also put in place to lower risk and make sure that security standards were followed in the organization..

2. Purpose of Using A-SMS, A-GW, and A-GUI

Check Point uses a centralized management architecture that separates management, enforcement, and administration duties to make things safer and easier to grow.

A-SMS (Security Management Server)

The A-SMS controls the whole Check Point environment from one place. It keeps track of all the security policies, firewall rules, network objects, user definitions, logs, and licensing information. Centralized management makes it easier for the whole company to run, speeds up audits, and makes sure that policies are followed in the same way across the board.

A-GW (Security Gateway)

The A-GW is in charge of making sure that the A-SMS's security rules are followed. It looks at network traffic, lets in connections that are allowed, stops illegal access, and protects internal networks from threats from outside. Separating the gateway from the management server improves performance and lowers the attack surface.

A-GUI (Management Workstation)

The administrator uses SmartConsole, which has a graphical user interface for managing the security infrastructure, on the A-GUI workstation. This secure management endpoint is where all policy setup, monitoring, and licensing tasks take place.

These parts work together to make a best practice enterprise firewall architecture.

3. Deployment Order and Methodology

To ensure a stable and logical deployment, the components were configured in the following order:

1. **A-SMS** – to establish the central management server first
2. **A-GUI** – to install SmartConsole for administration
3. **A-GW** – to register and manage the gateway through A-SMS

This approach ensured that management services were fully operational before adding the gateway.

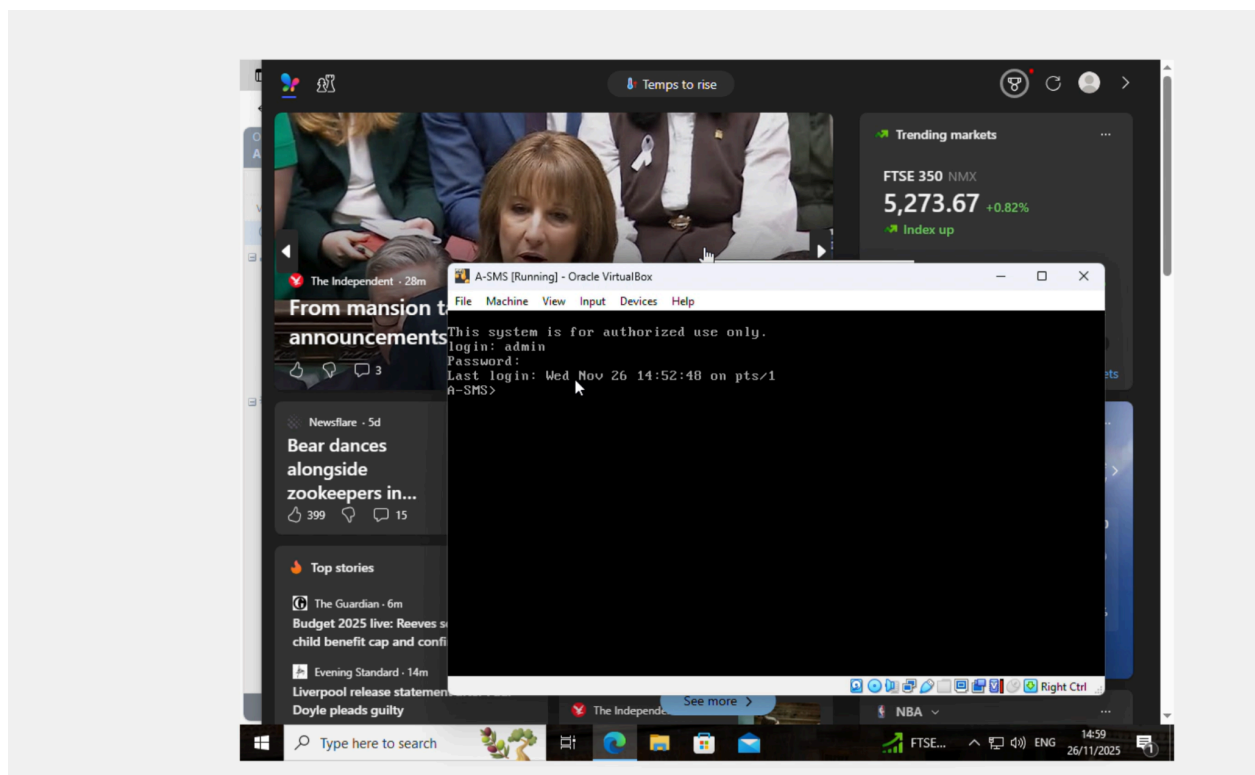
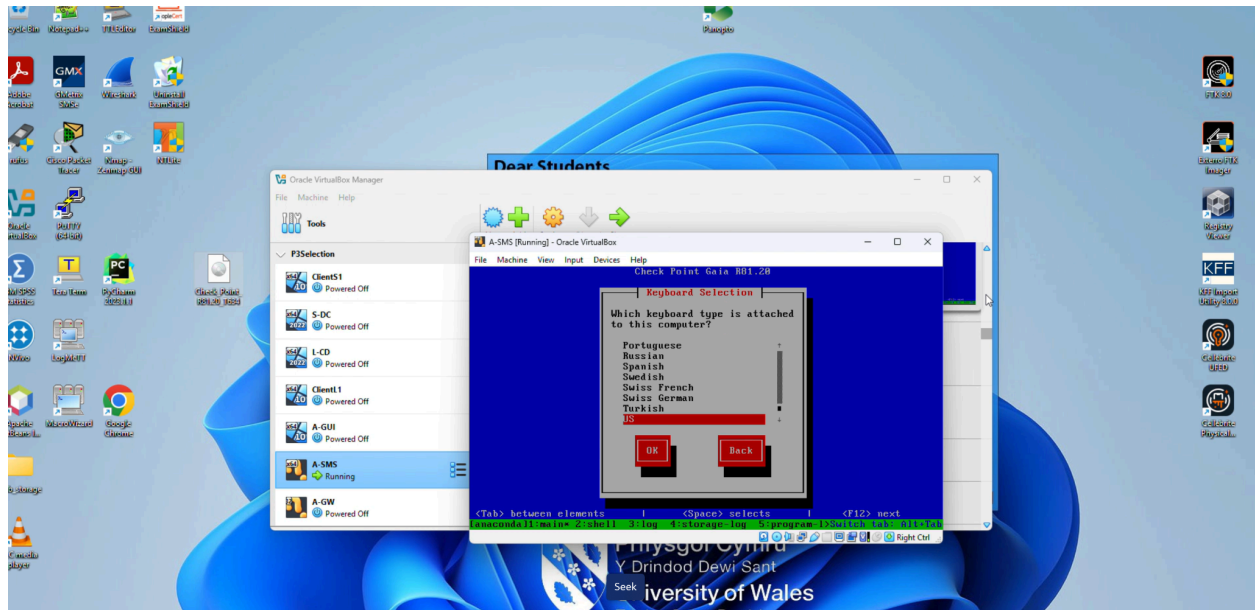
4. A-SMS Configuration (Security Management Server)

The A-SMS was installed and configured using the Gaia First Time Configuration Wizard.

Configuration Details

- **Device Name:** A-SMS
- **IPv4 Address:** 10.1.1.101
- **Operating System:** Gaia
- **Version:** R81.20
- **Administrator Account:** admin

Setting up the system included choosing a keyboard, giving it an IP address, setting up the management interface, and making an administrator password. After it was finished, HTTPS was used to make sure that the Gaia Web UI could be accessed.



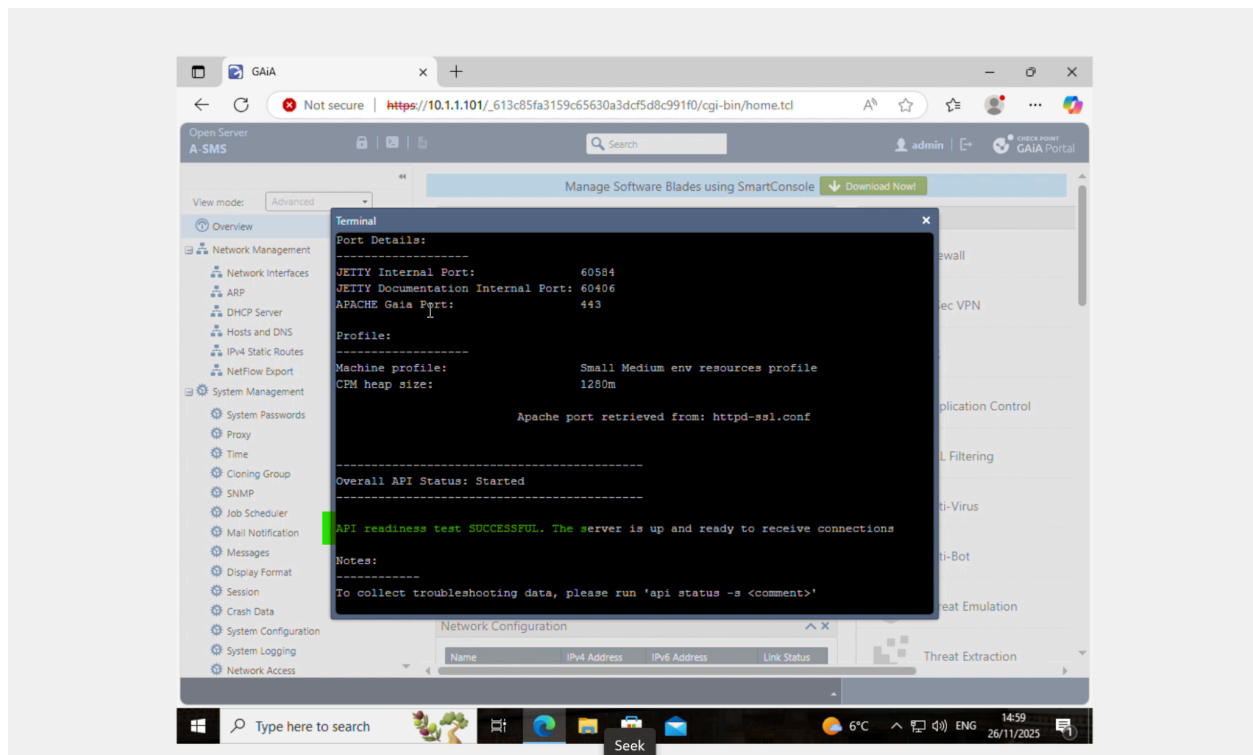
5. Troubleshooting A-SMS Status Failure

The A-SMS showed a failure status after the first setting, which stopped normal management tasks. Instead of reinstalling the system, they did some troubleshooting.

Troubleshooting Actions

- Logged into the Gaia CLI as admin
- Verified management and API services
- Adjusted session and inactivity timeout values
- Saved the configuration
- Rechecked system readiness

After doing these things, the system confirmed that management services were working by reporting a successful API readiness status.



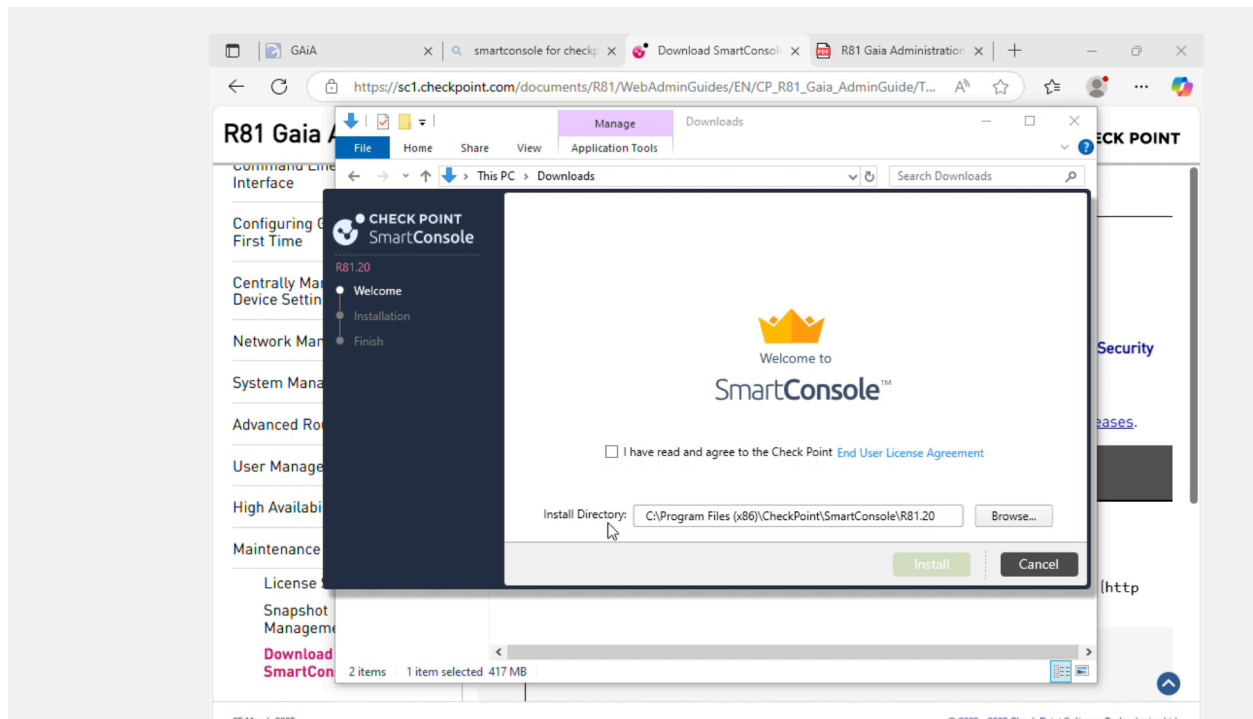
6. SmartConsole Installation on A-GUI

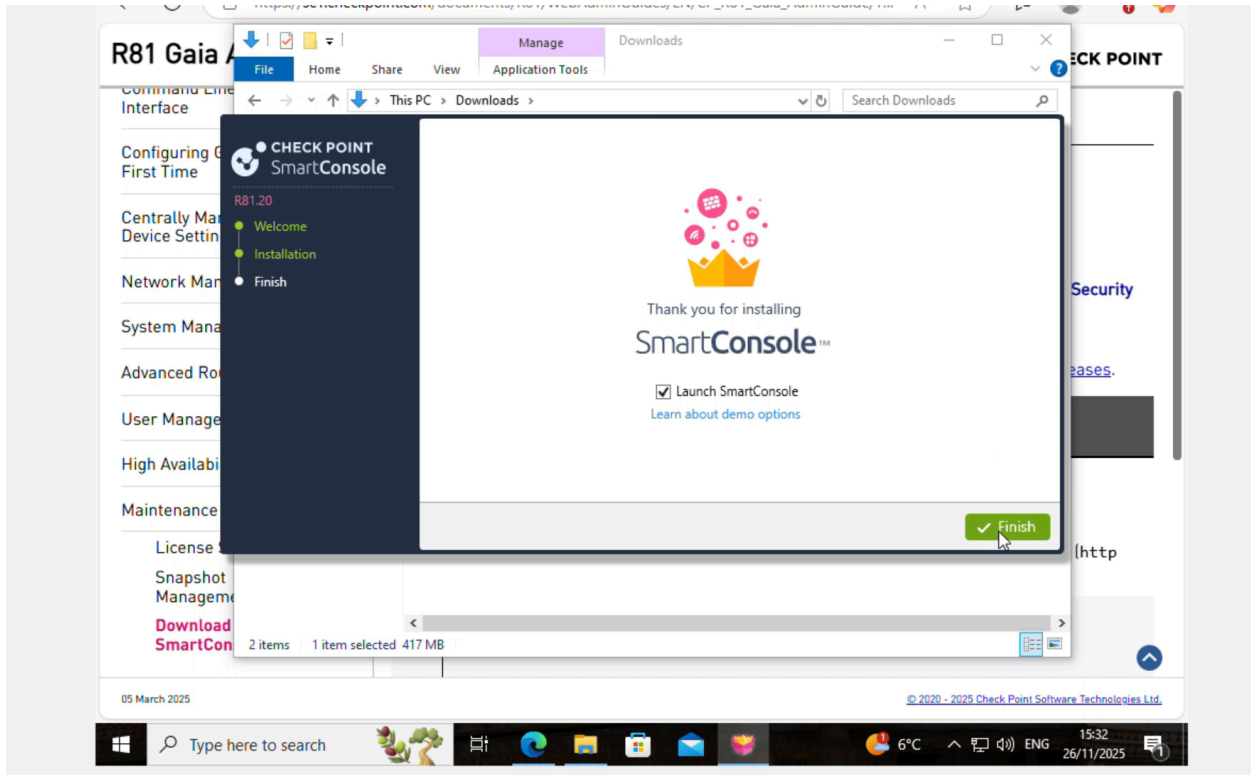
To centrally manage the Check Point environment, SmartConsole R81.20 was installed on the A-GUI workstation.

The installation process included:

- Accepting the Check Point End User License Agreement
- Selecting the installation directory
- Completing installation and launching SmartConsole

After installation, SmartConsole was used to connect to the A-SMS at IP address 10.1.1.101.





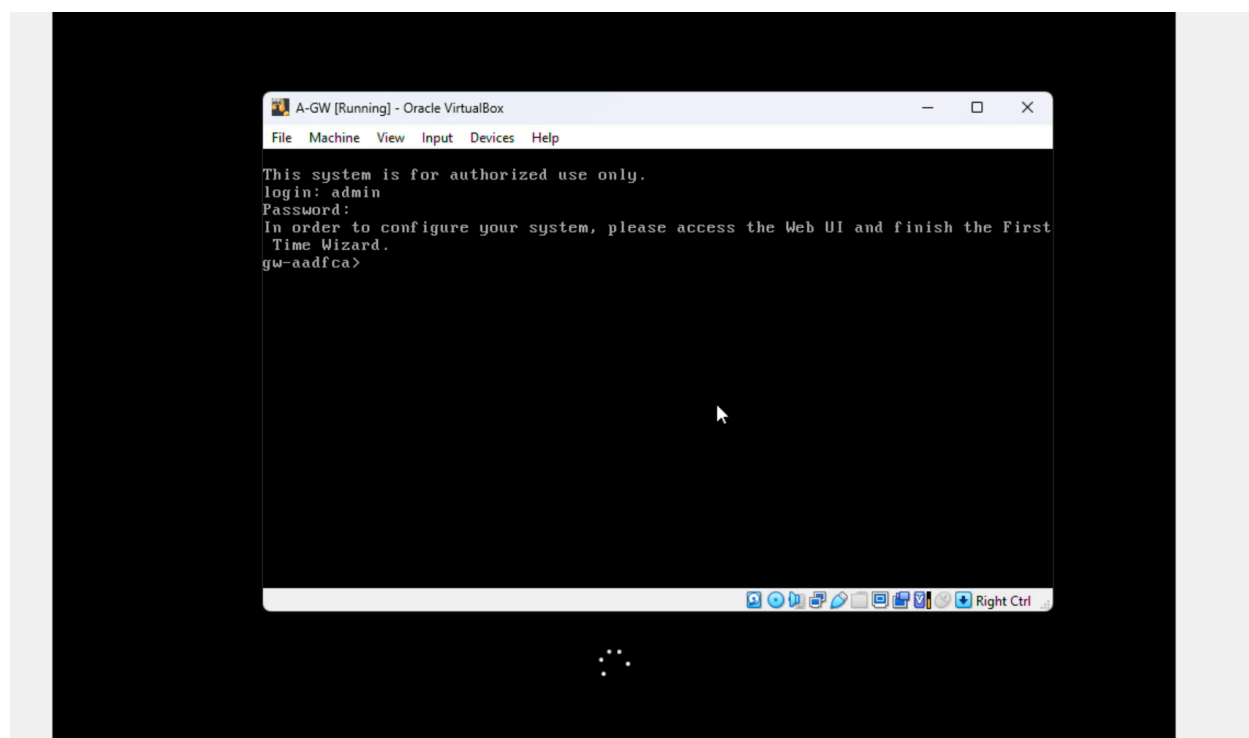
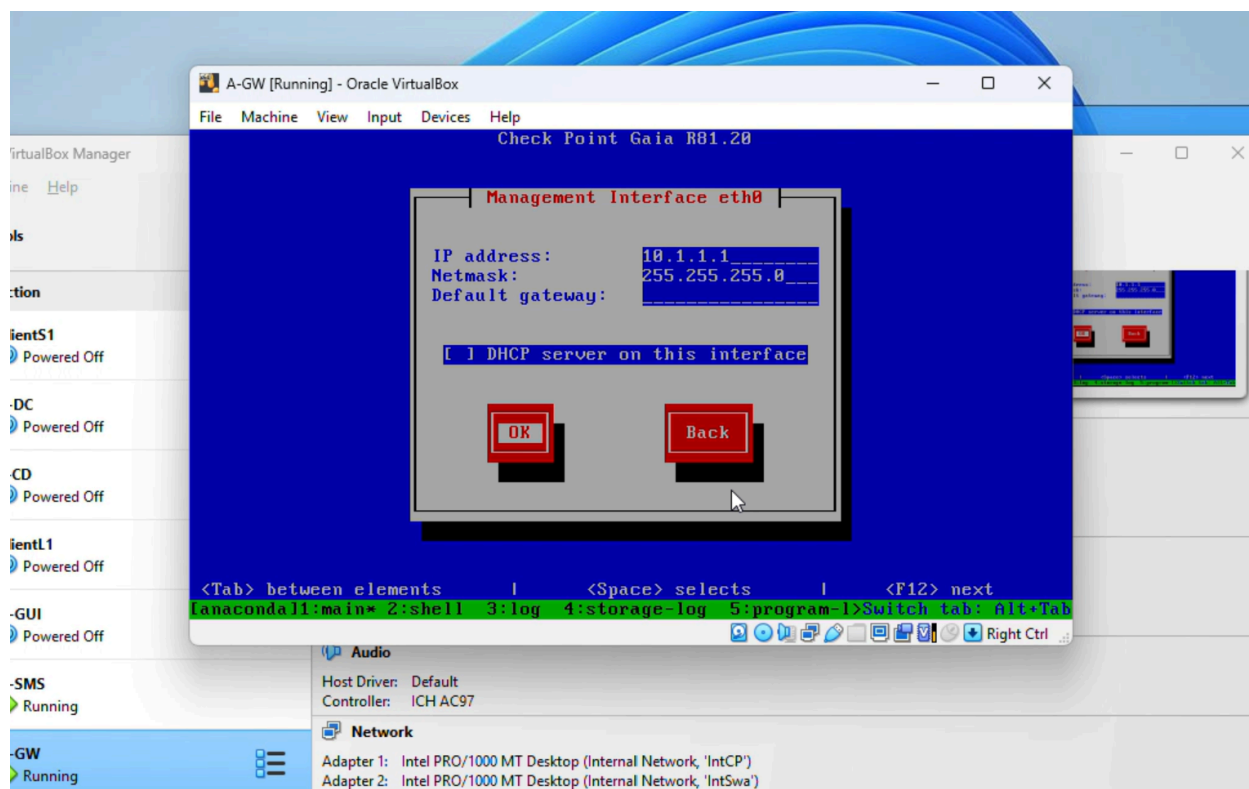
7. A-GW Configuration (Security Gateway)

Once A-SMS and SmartConsole were operational, the A-GW was configured.

Configuration Details

- **Device Name:** A-GW
- **IPv4 Address:** 10.1.1.1
- **Operating System:** Gaia
- **Version:** R81.20

We used the Gaia setup interface to set up the gateway. A-GW and A-SMS were able to set up Secure Internal Communication (Trust) after making the gateway object in SmartConsole.

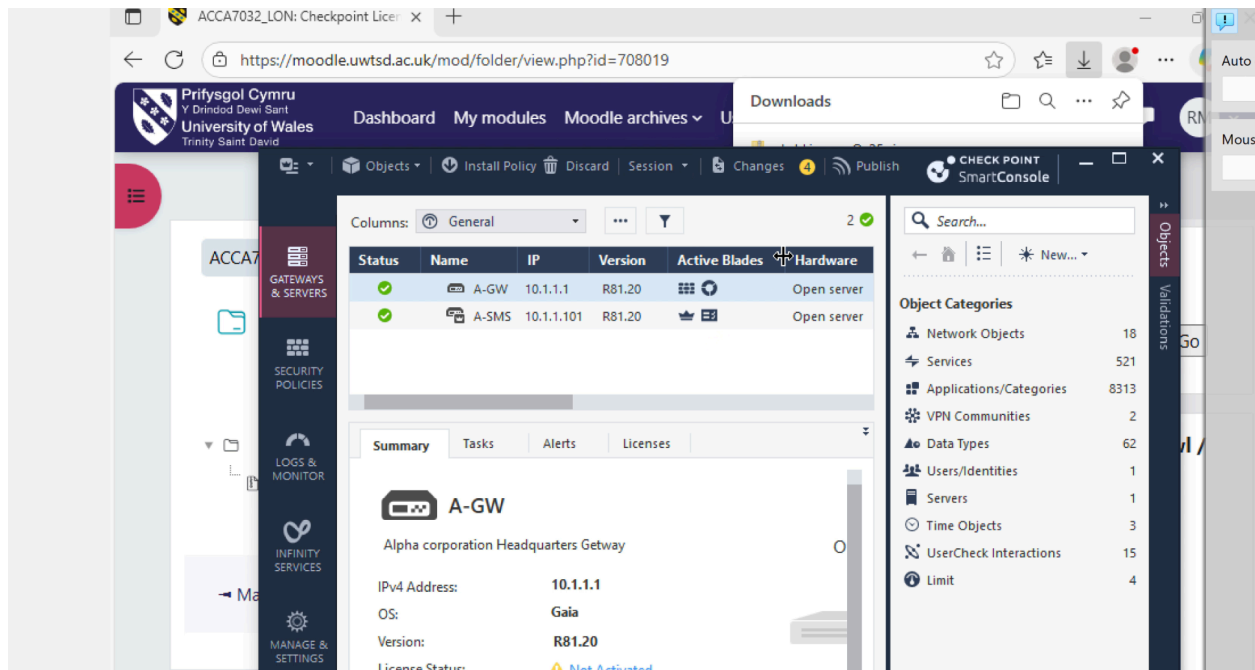


8. Verification of Connectivity (Swansea Network ↔ A-SMS)

After configuration, both devices appeared correctly in SmartConsole:

- **A-SMS – 10.1.1.101**
- **A-GW – 10.1.1.1**

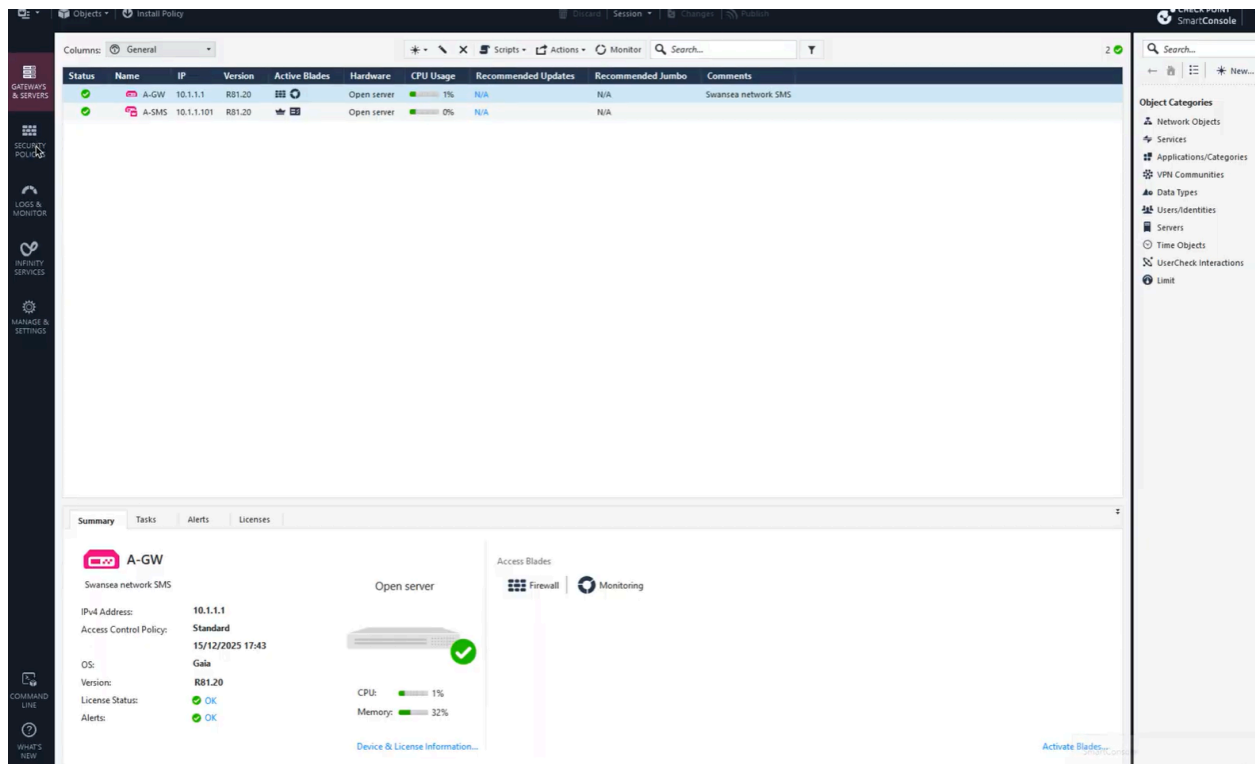
Both showed green status indicators, confirming successful communication and centralized management. API readiness tests further confirmed operational status.



9. Licensing Configuration and Verification

We followed Check Point's rules and applied for and got a license. The license status and contract details were checked to make sure that the module criteria were being met.

The licensing screens check to see if the gateway and management server meet the requirements for a license.



10. Enterprise Firewall Policy Design (Justification)

In a real enterprise environment, firewall rules should follow the **principle of least privilege**, meaning that:

- Only required services are allowed
- Management access is restricted to trusted hosts
- All other traffic is explicitly denied

For this implementation:

- Administrative access is allowed only from the A-GUI management workstation
- Management services such as SSH and ICMP are controlled and logged
- A cleanup rule is applied to block all unspecified traffic

This approach reduces the attack surface and ensures accountability through logging.

11. Firewall Rules Configuration

Firewall rules were created in **Access Control** → **Policy** within SmartConsole.

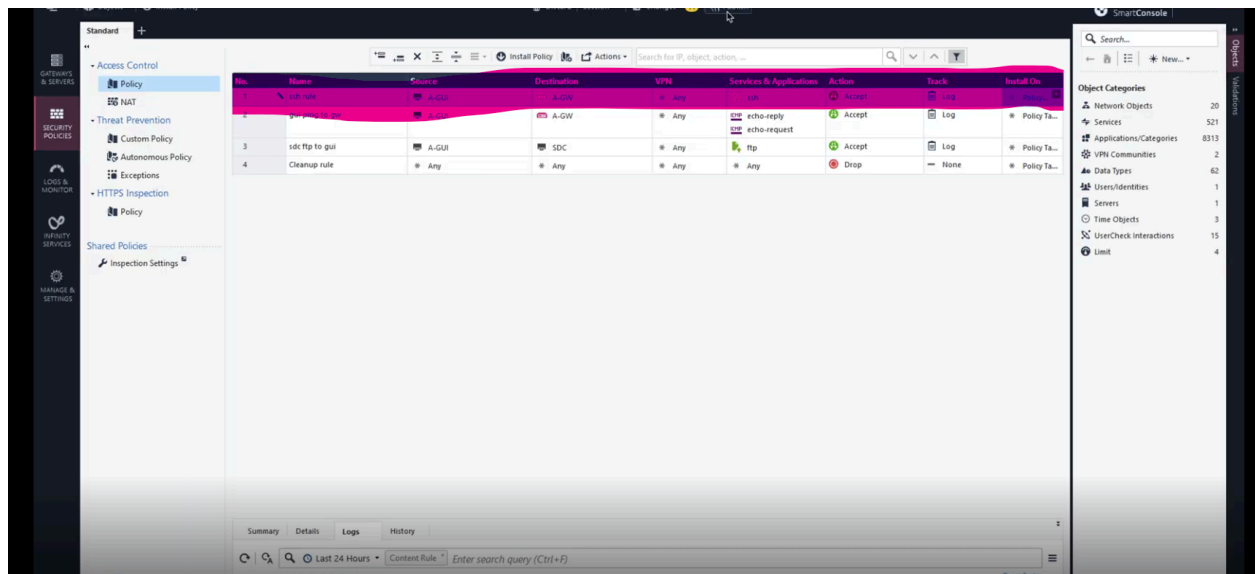
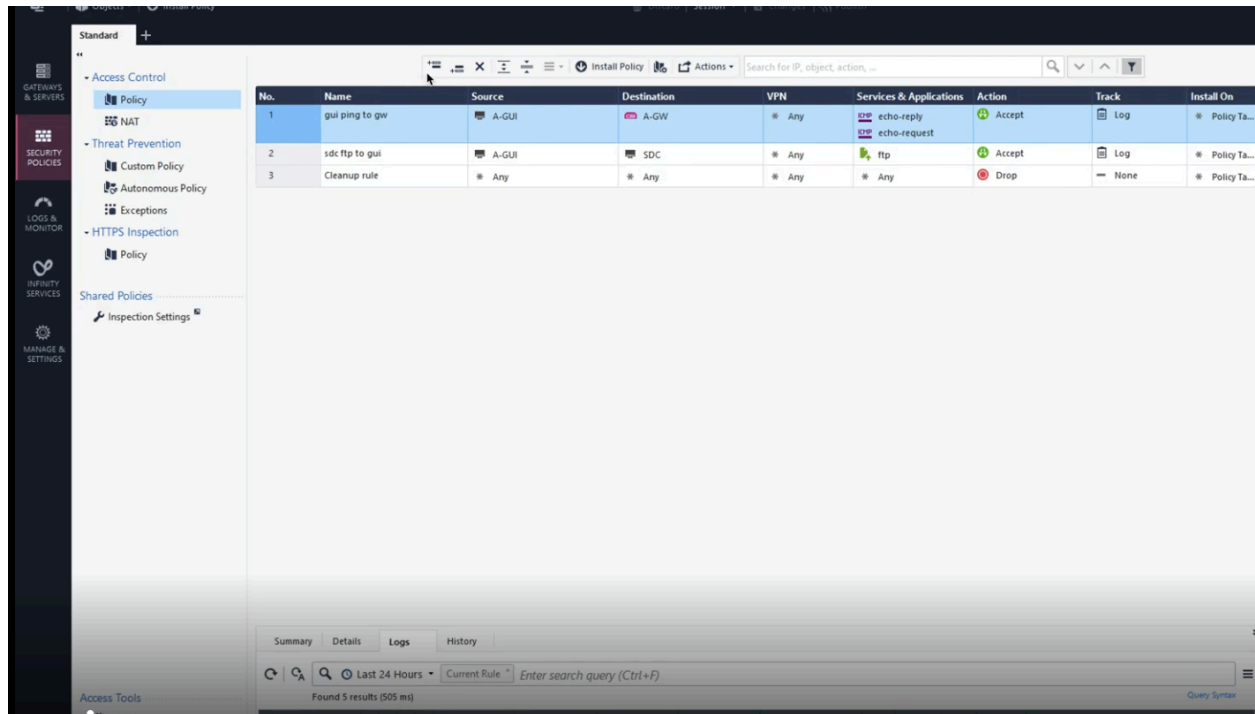
11.1 SSH Access Rule (Remote Administration)

An SSH rule was configured to allow secure remote access to the gateway for administration.

Rule Details:

- **Source:** A-GUI
- **Destination:** A-GW
- **Service:** SSH
- **Action:** Accept
- **Tracking:** Log

This ensures that only the authorized management workstation can access the gateway via SSH.



11.2 ICMP (Ping) Rule – Connectivity Verification

ICMP traffic was allowed from A-GUI to A-GW to enable connectivity testing and troubleshooting.

Rule Details:

- **Source: A-GUI**

- **Destination:** A-GW
- **Service:** ICMP (echo-request / echo-reply)
- **Action:** Accept
- **Tracking:** Log

The screenshot shows the Palo Alto Networks Security Policy configuration interface. The left sidebar contains navigation options: Gateways & Servers, Security Policies, Logs & Monitor, Infinity Services, and Manage & Settings. The main pane displays a table of security rules under the 'Standard' tab.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	gui ping to gw	A-GUI	A-GW	Any	icmp-echo-reply, icmp-echo-request	Accept	Log	Policy Ta...
2	sdic ftp to gui	A-GUI	SDC	Any	ftp	Accept	Log	Policy Ta...
3	Cleanup rule	Any	Any	Any	Any	Drop	None	Policy Ta...

At the bottom, there are tabs for Summary, Details, Logs, and History. A search bar is visible with the text 'Found 5 results (505 ms)'.

This screenshot shows the same Palo Alto Networks Security Policy configuration interface as the first image, but with a Command Prompt window overlaid in the foreground. The Command Prompt shows the results of a ping command to 10.1.1.1, indicating successful connectivity.

```

Microsoft Windows [Version 10.0.19045.5854]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin\ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:
Reply from 10.1.1.1: bytes=32 time=4ms TTL=64
Reply from 10.1.1.1: bytes=32 time=2ms TTL=64
Reply from 10.1.1.1: bytes=32 time=2ms TTL=64

```

The background interface shows the same security rule table as before, with the 'gui ping to gw' rule highlighted.

This confirms that the firewall policy allows ICMP traffic only from trusted sources.

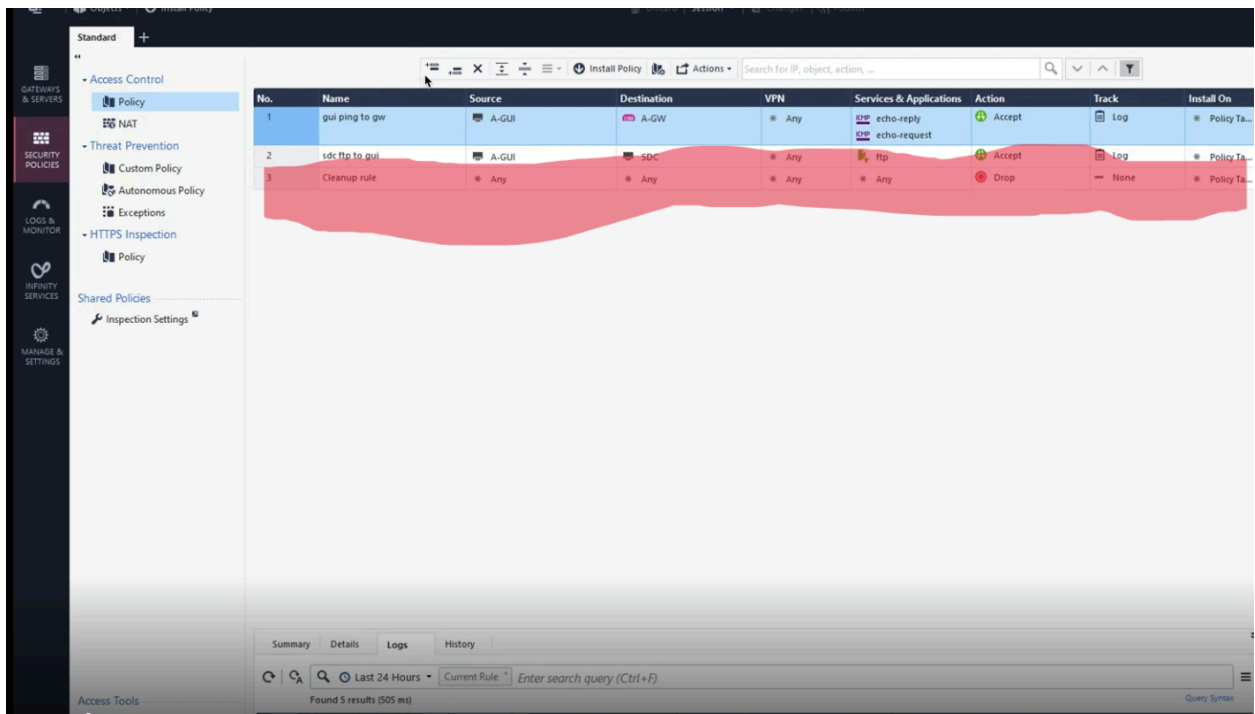
11.3 Cleanup Rule (Default Deny)

A cleanup rule was added at the bottom of the policy to block all remaining traffic.

Rule Details:

- **Source:** Any
- **Destination:** Any
- **Service:** Any
- **Action:** Drop
- **Tracking:** None

This rule ensures that any traffic not explicitly allowed is denied, which is a core enterprise firewall best practice.



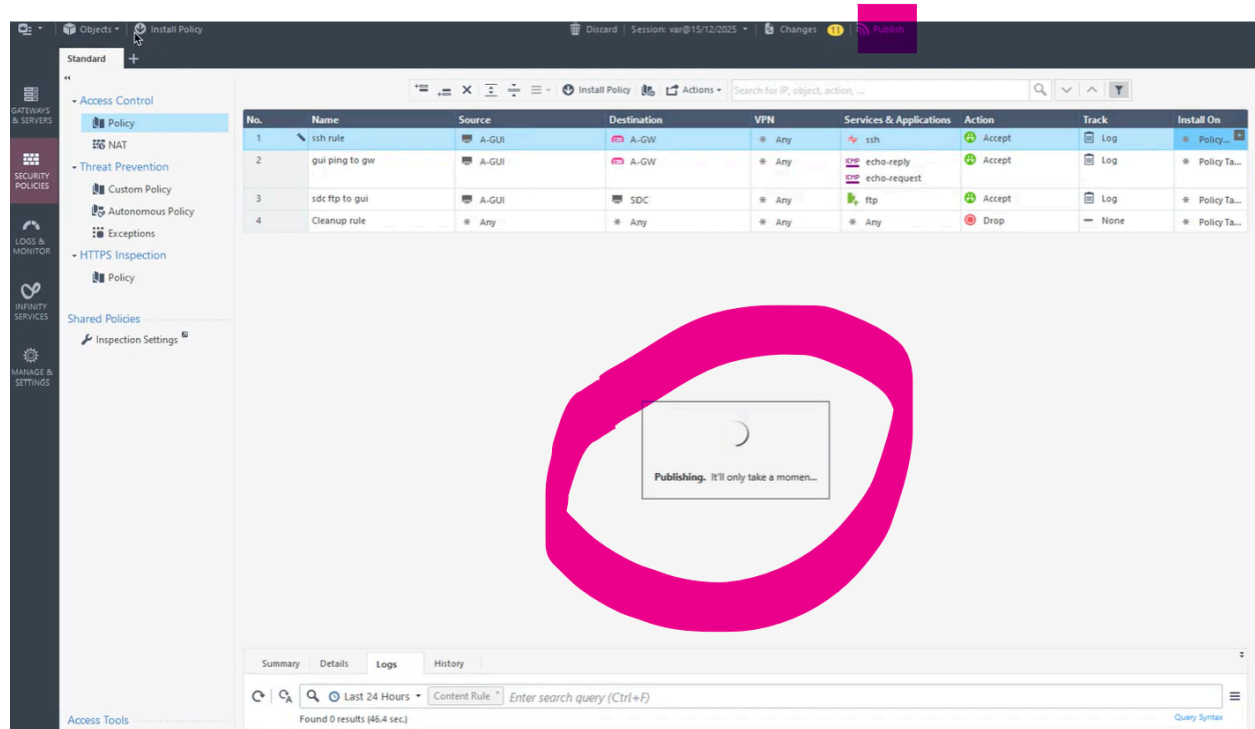
The screenshot displays the Palo Alto Networks firewall configuration interface. On the left, a sidebar shows navigation options: Gateways & Servers, Security Policies, Logs & Monitor, Infinity Services, and Manage & Settings. The 'Security Policies' section is expanded, showing 'Access Control' and 'Threat Prevention'. The 'Access Control' section is further expanded, showing 'Policy', 'NAT', 'Custom Policy', 'Autonomous Policy', 'Exceptions', 'HTTPS Inspection', and 'Policy'. The 'Policy' section is selected, and the 'Standard' tab is active. The main area shows a table of policies. The table has columns: No., Name, Source, Destination, VPN, Services & Applications, Action, Track, and Install On. Three policies are listed: 1. 'gui ping to gw' (Source: A-GUI, Destination: A-GW, Action: Accept, Track: Log), 2. 'sid ftp to gui' (Source: A-GUI, Destination: SDC, Action: Accept, Track: Log), and 3. 'Cleanup rule' (Source: Any, Destination: Any, Action: Drop, Track: None). The 'Cleanup rule' is highlighted in red. Below the table, there are tabs for 'Summary', 'Details', 'Logs', and 'History'. The 'Logs' tab is selected, showing a search bar and a 'Found 5 results (505 ms)' message.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	gui ping to gw	A-GUI	A-GW	Any	echo-reply, echo-request	Accept	Log	Policy Ta...
2	sid ftp to gui	A-GUI	SDC	Any	ftp	Accept	Log	Policy Ta...
3	Cleanup rule	Any	Any	Any	Any	Drop	None	Policy Ta...

12. Policy Installation and Enforcement

The policy was made public, the firewall rules were set up, and then the A-GW was put in place.

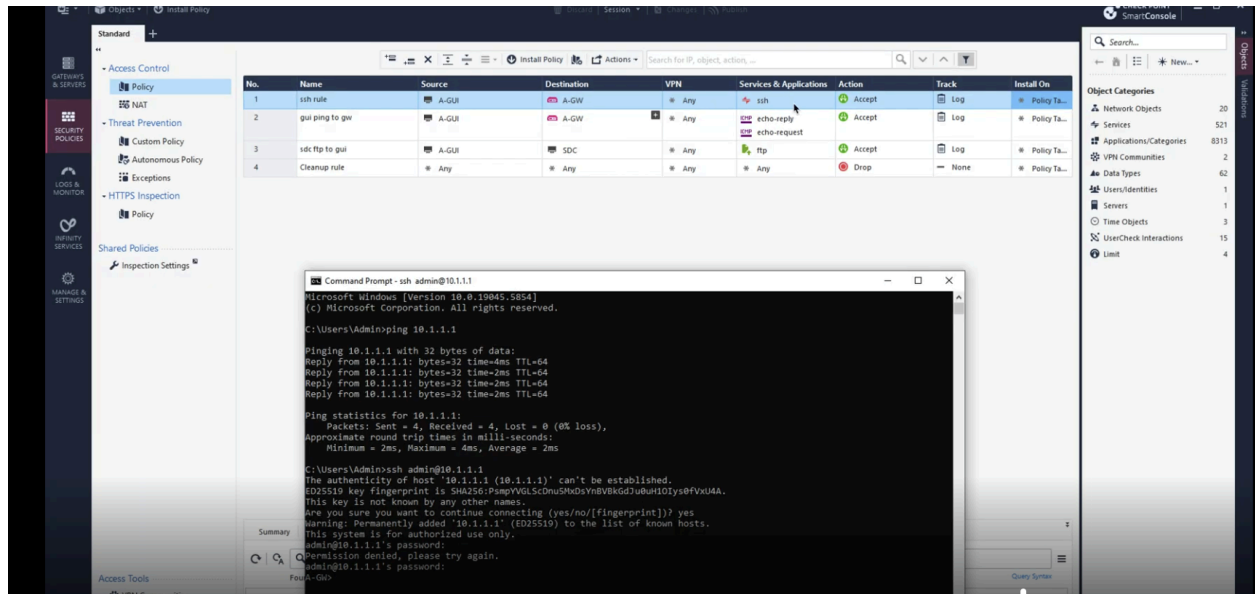
When you install the policy, it puts the rules on the gateway; when you publish the changes, they are saved in the management database.



13. Verification of Remote Access (SSH)

To verify that the firewall rules were working as intended, a remote SSH connection was initiated from the management workstation to the gateway.

- SSH access was successful
- Authentication was required
- Connection was logged



This confirms that the SSH rule is functioning correctly and that unauthorized access is blocked by default.

14. Administrator and User Access Control

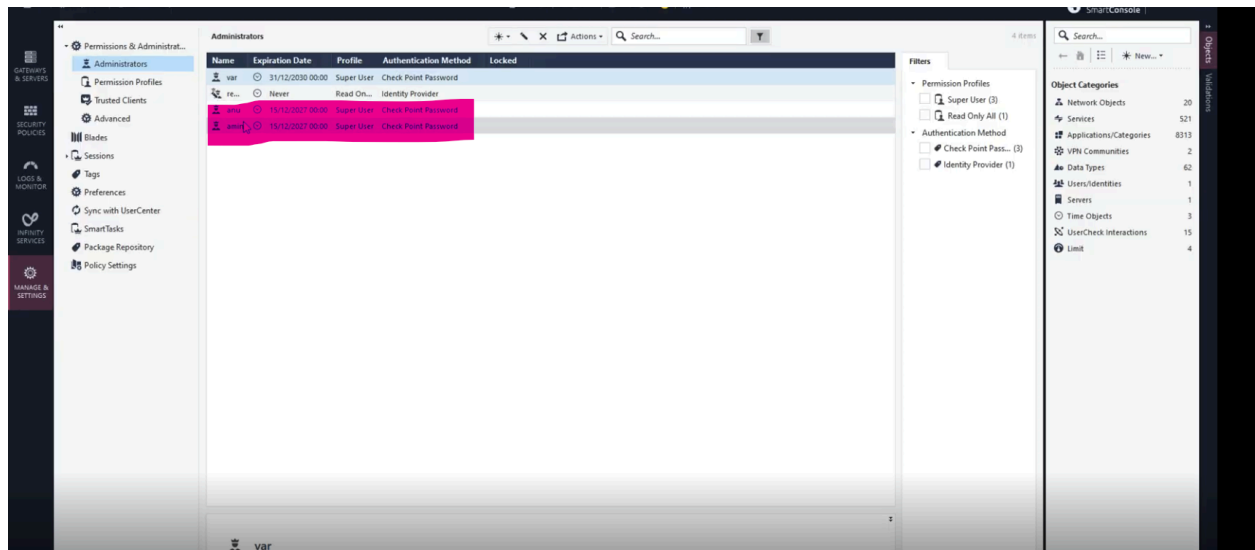
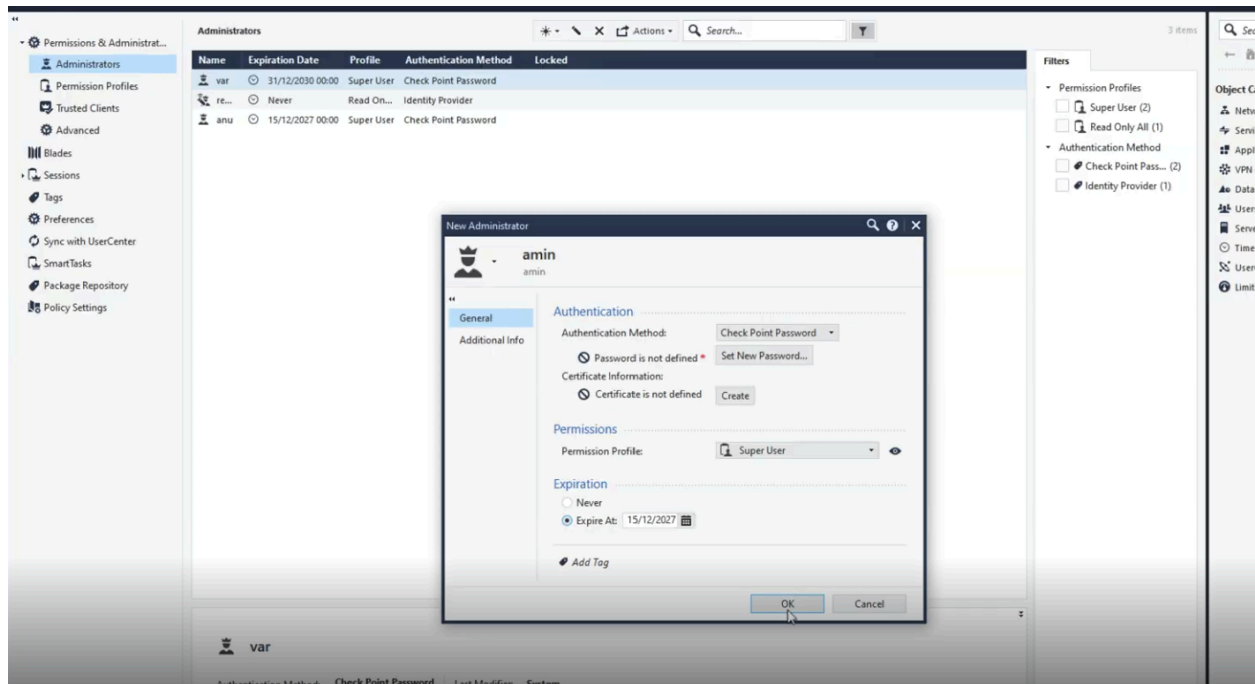
To improve management security, additional administrators were created with defined roles and expiration settings.

14.1 Creating New Administrator Accounts

A new administrator account was created to demonstrate controlled administrative access instead of relying solely on the default admin account.

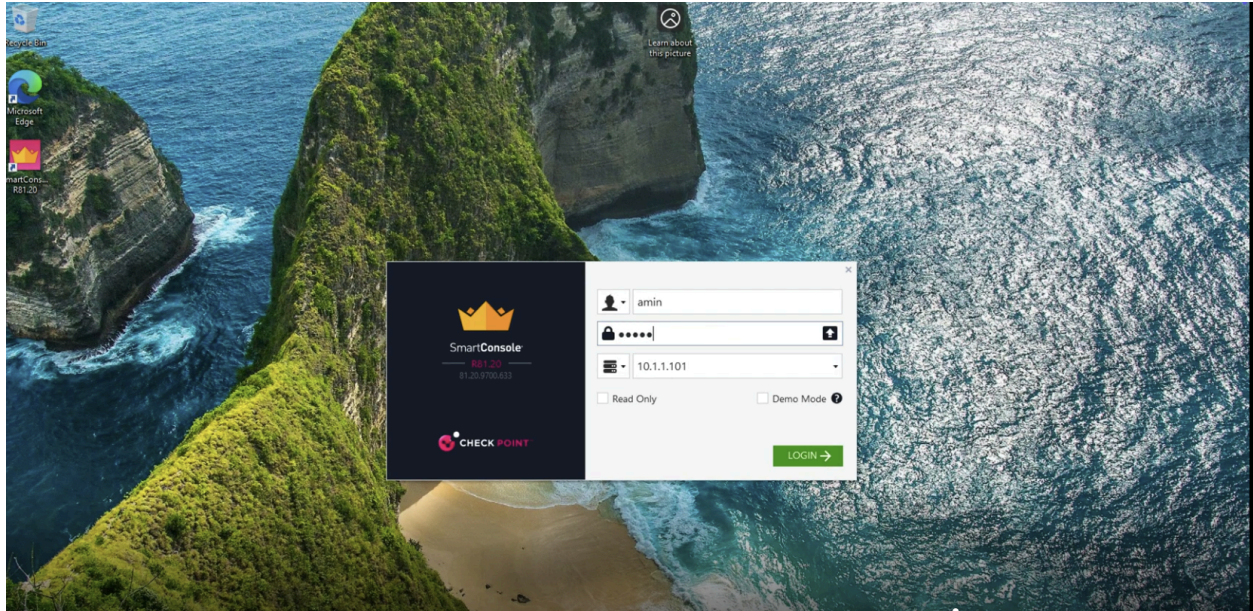
Security Measures Applied:

- Unique administrator username
- Check Point password authentication
- Role-based permissions (Super User / Read-Only)
- Account expiration date configured



14.2 Logging in Using New Administrator

To verify that the new administrator account works correctly, SmartConsole login was performed using the newly created credentials.



This confirms that role-based administrator access is functional and secure.

15. Security Benefits of Role-Based Administration

Implementing multiple administrator accounts provides the following benefits:

- Reduces reliance on a single admin account
- Improves accountability and auditing
- Limits damage if credentials are compromised
- Aligns with enterprise security standards (ISO 27001 principle of least privilege)

16. Additional Security Enhancements (Alignment with Standards)

The implemented controls align with recognized security best practices, including:

- **Least privilege access control**
- **Separation of management and enforcement**

- **Explicit allow rules with default deny**
- **Logging of administrative actions**

These measures significantly improve the security posture of the enterprise network.

17. Conclusion

The solution that was put in place shows a full and professionally designed enterprise security architecture that uses Check Point technology. Centralized security management was successfully set up, which made it possible to apply policies consistently, make administration easier, and keep an eye on the whole network.

The firewall's rules were carefully made to stop illegal traffic from entering and leaving the system. This was done by only allowing necessary services from trusted sources and blocking all other connections. During the deployment and testing of the policy, it was confirmed that the access control rules were put into place correctly and that management connectivity worked as planned.

Adding more security features, like role-based administrative access and controlled management authentication, made the network's security even stronger. By putting these measures in place, administrative risk was lowered, accountability was raised, and the implementation was in line with established industry standards like least privilege and separation of duties.

Overall, the solution provides a secure, scalable, and well-managed business network that follows best practices for security in the real world and shows how to use Check Point Gaia appliances effectively to protect a business network.