

**Enterprise Network Security Implementation and
Policy Enforcement Using Check Point
SmartConsole**

Student Name:	MD Monsuruzzaman
Student ID:	2504658
Programme:	MSc Cybersecurity and Digital Forensics
Institution:	University of Wales Trinity Saint David London
Module:	Enterprise Network Security
Module Code:	ACCA7032
Lecturer:	Renuga Jayakumar
Submission Date:	14th August 2026

Table of Content

Introduction.....	3
1. Enterprise Network Architecture.....	3
1. Enterprise Network Architecture.....	3
2. SmartConsole Authentication.....	4
3. Gateway and Management Server Configuration.....	5
4. Device Status Verification.....	6
5. Licensing Verification.....	8
6. Network Object Configuration.....	8
7. Firewall Policy Configuration.....	9
8. Policy Installation.....	11
9. Restricted User Group Configuration.....	12
10. Traffic Verification.....	14
11. Log Monitoring.....	16
11. Evaluation.....	18
12. Conclusion.....	18

Introduction

Enterprise network security is a fundamental component of modern organisational infrastructure. A Security Management Server (A-SMS) provides centralised administration while a Security Gateway (A-GW) enforces access control policies between trusted internal networks and untrusted external networks. Check Point SmartConsole enables administrators to configure gateways, create security policies, deploy rule bases, monitor traffic, and analyse logs from a single interface [1], [2]. This report documents the practical implementation of an enterprise firewall environment using Check Point SmartConsole, including gateway verification, policy configuration, policy installation, traffic validation, and log monitoring. The objective of the exercise was to demonstrate secure network segmentation, least-privilege access control, and centralised firewall management.

1. Enterprise Network Architecture

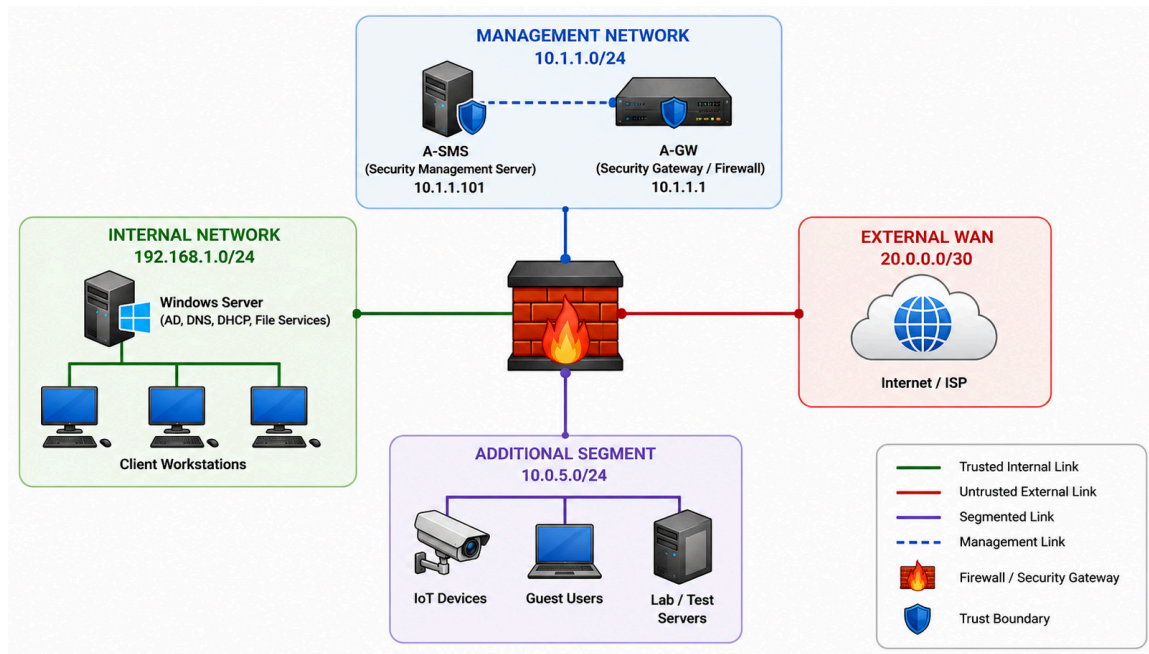


Figure 1. Enterprise Network Security Architecture

1. Enterprise Network Architecture

The architecture demonstrates network segmentation by separating management, internal, additional segment, and external WAN networks. Segmentation limits lateral movement and reduces the attack surface, while the Security Gateway controls traffic crossing trust boundaries [3], [5].

2. SmartConsole Authentication

Administrator authentication ensures that only authorised users can modify firewall policies. SmartConsole provides role-based administrative control and secure communication with the management server before configuration changes are deployed [1].

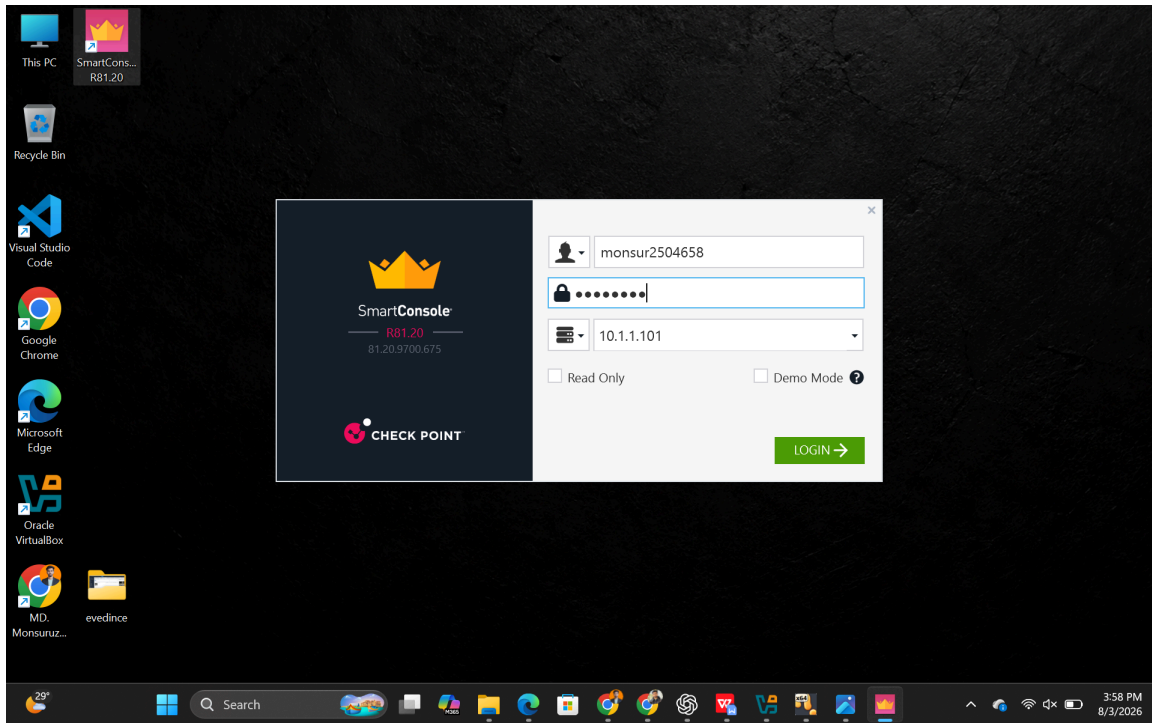


Figure 2. SmartConsole Login Interface Showing Administrator Username

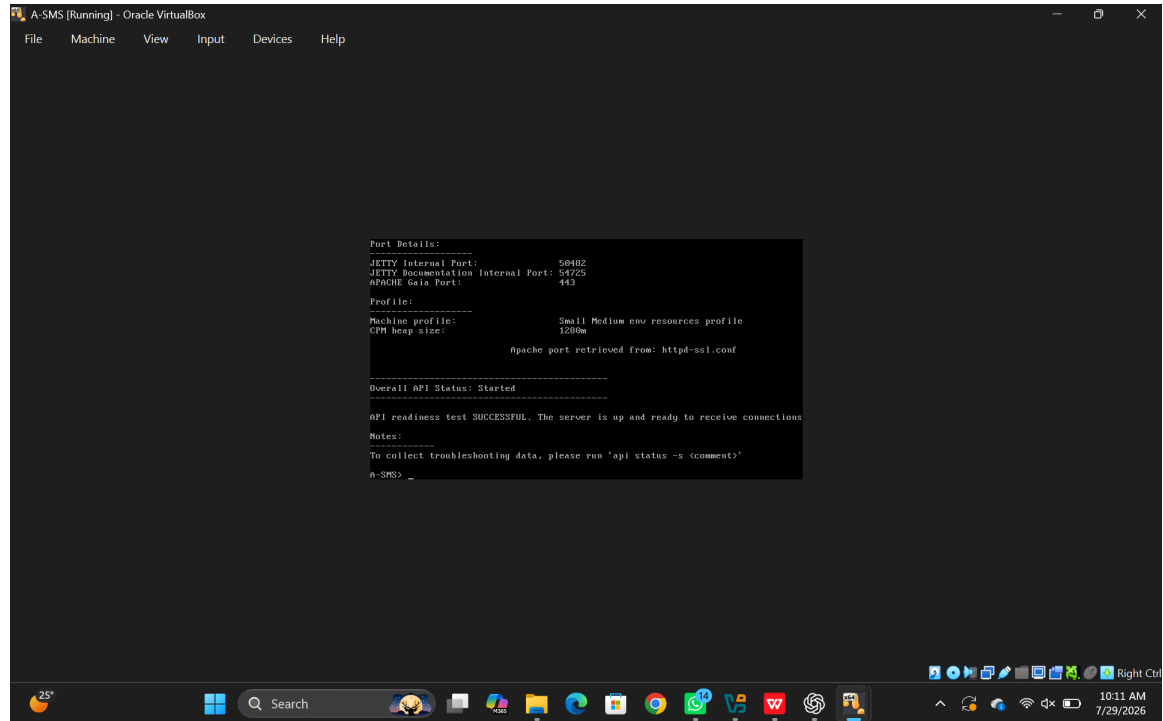


Figure 3. A-SMS API Status Verification

3. Gateway and Management Server Configuration

A secure trust relationship between the Security Management Server (A-SMS) and Security Gateway (A-GW) is required before policies can be installed. The gateway must be reachable and correctly configured so that compiled rule bases can be enforced consistently across the network. After verifying the S-DC firewall settings, communication between A-SMS and A-GW was confirmed and the management connection was successfully established.

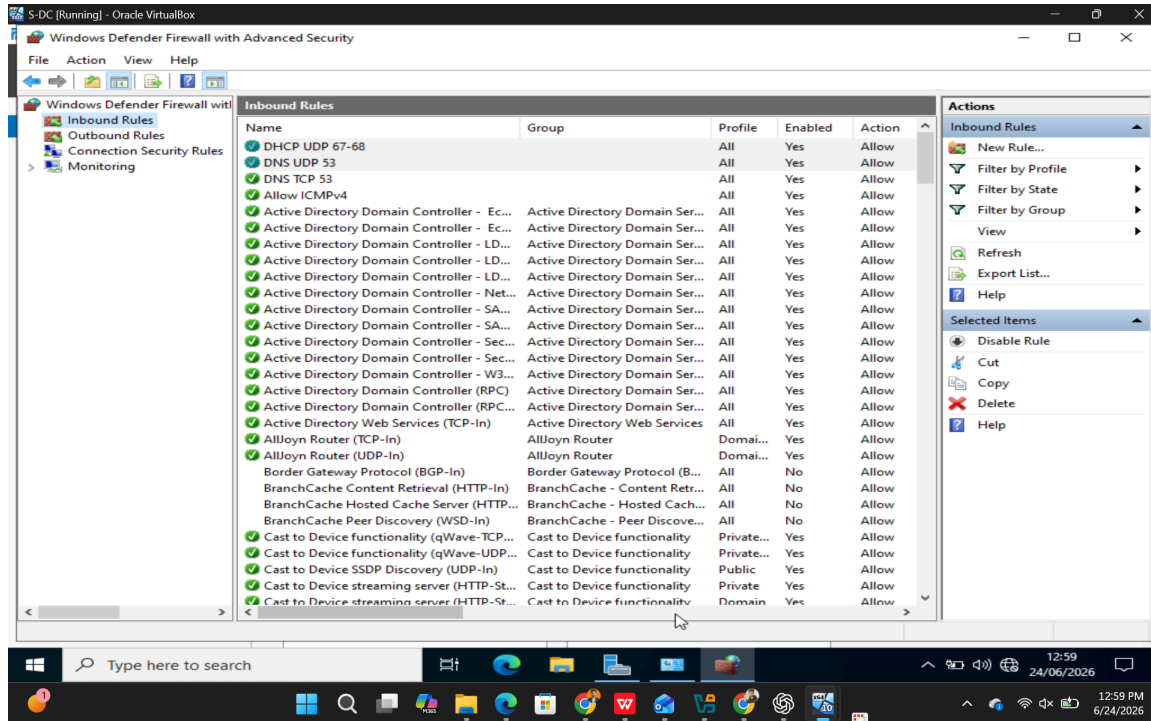


Figure 4. Windows Defender Firewall with Advanced Security on S-DC

The screenshot shows the Windows Defender Firewall with Advanced Security interface on the S-DC server, where inbound firewall rules were reviewed to ensure that required network services were enabled before testing connectivity and firewall policies.

4. Device Status Verification

Device status verification confirmed that the Security Gateway (A-GW) was online, reachable, and operating normally. SmartConsole was used to monitor gateway communication, CPU usage, memory usage, and operational status to ensure that the gateway could receive policies from the Security Management Server (A-SMS) and enforce security controls reliably.

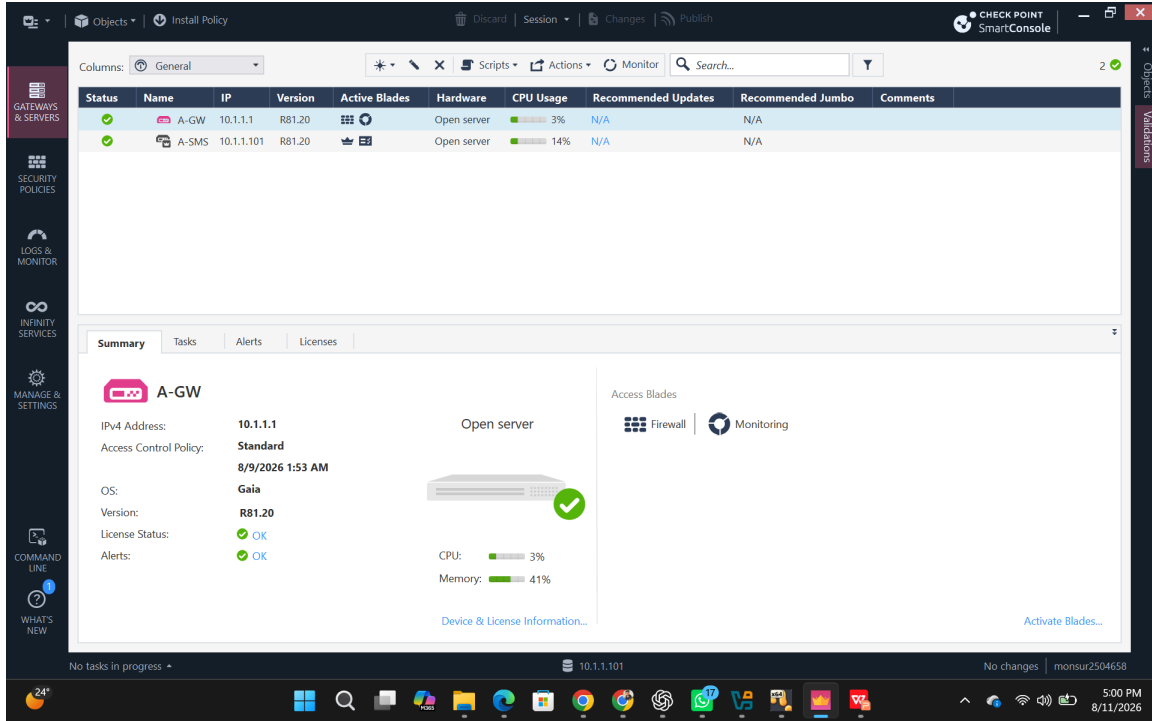


Figure 5. Device Status Verification of A-GW in SmartConsole

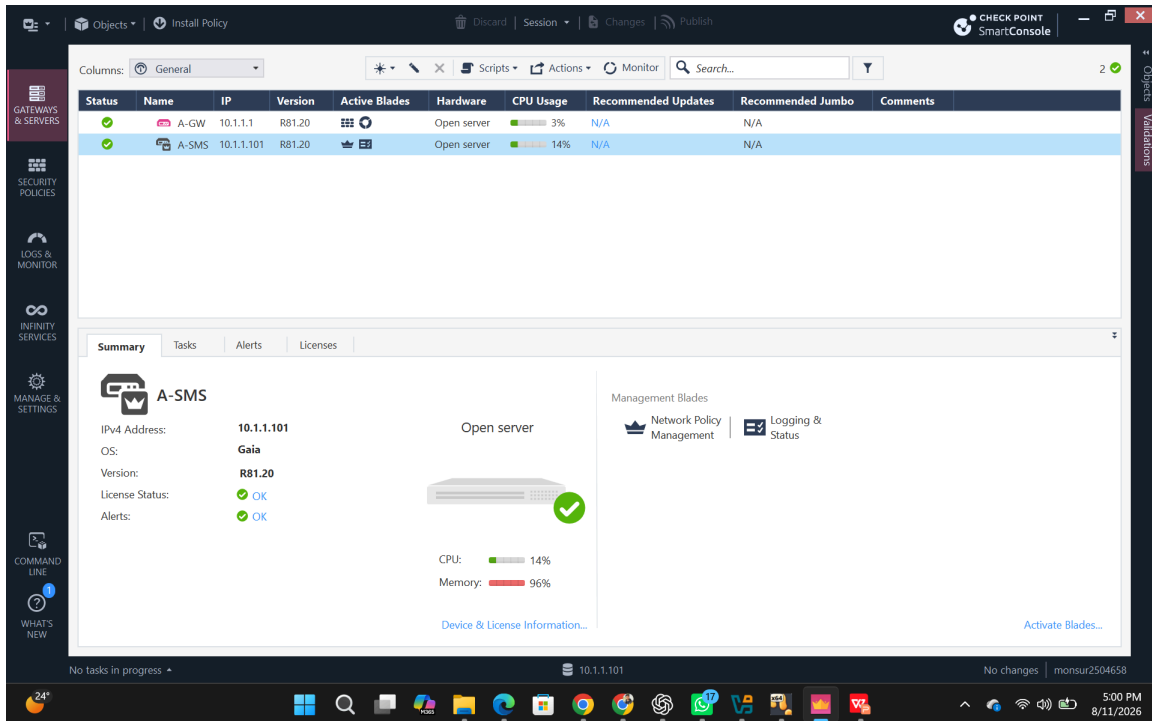


Figure 6. Device Status Verification of A-SMS in SmartConsole

5. Licensing Verification

The gateway licensing information was verified in SmartConsole to ensure that the Firewall and associated security blades were active and available for policy enforcement. Valid licensing confirms that enterprise security features can be applied without functional restrictions.

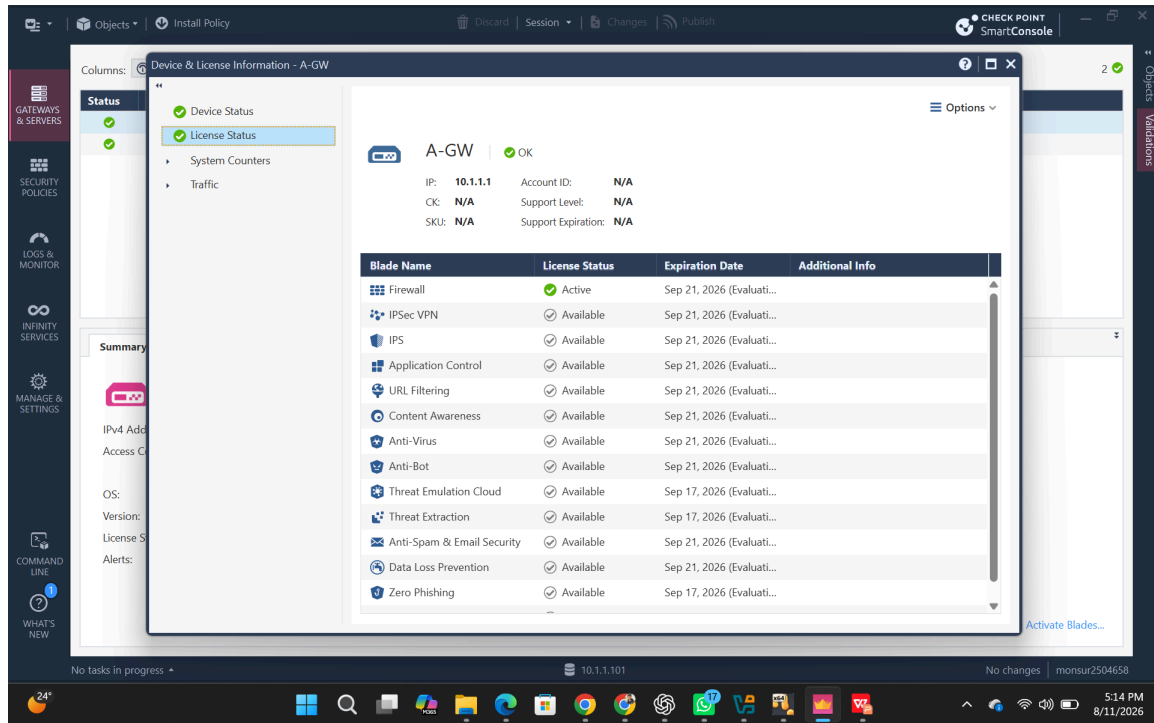


Figure 7. Licensing Verification

6. Network Object Configuration

A host object named Management_PC was created and assigned the appropriate management IP address. Object-based configuration simplifies policy management, improves rule readability, and allows reusable security policies across multiple network segments.

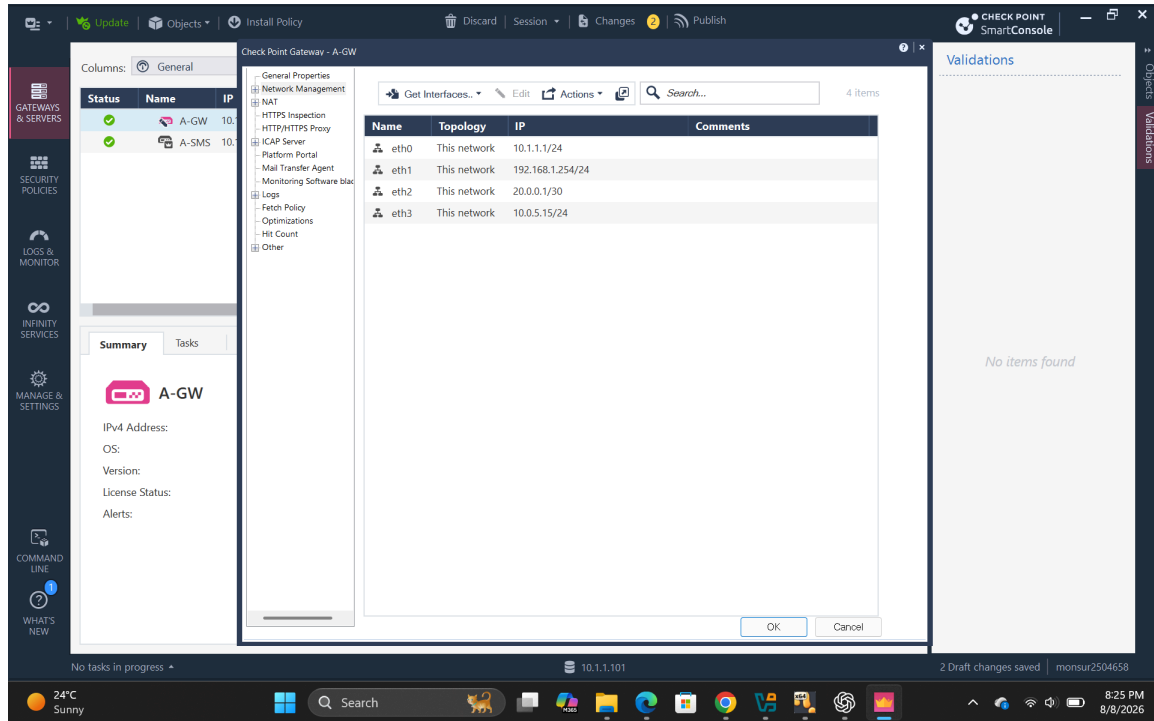


Figure 8. Network Object Configuration

7. Firewall Policy Configuration

HTTP and SSH were allowed to support testing and secure remote administration, while Telnet and FTP were blocked because they transmit credentials in plaintext. The rule set demonstrates the principle of least privilege and the use of logging for auditing and incident response [3], [4].

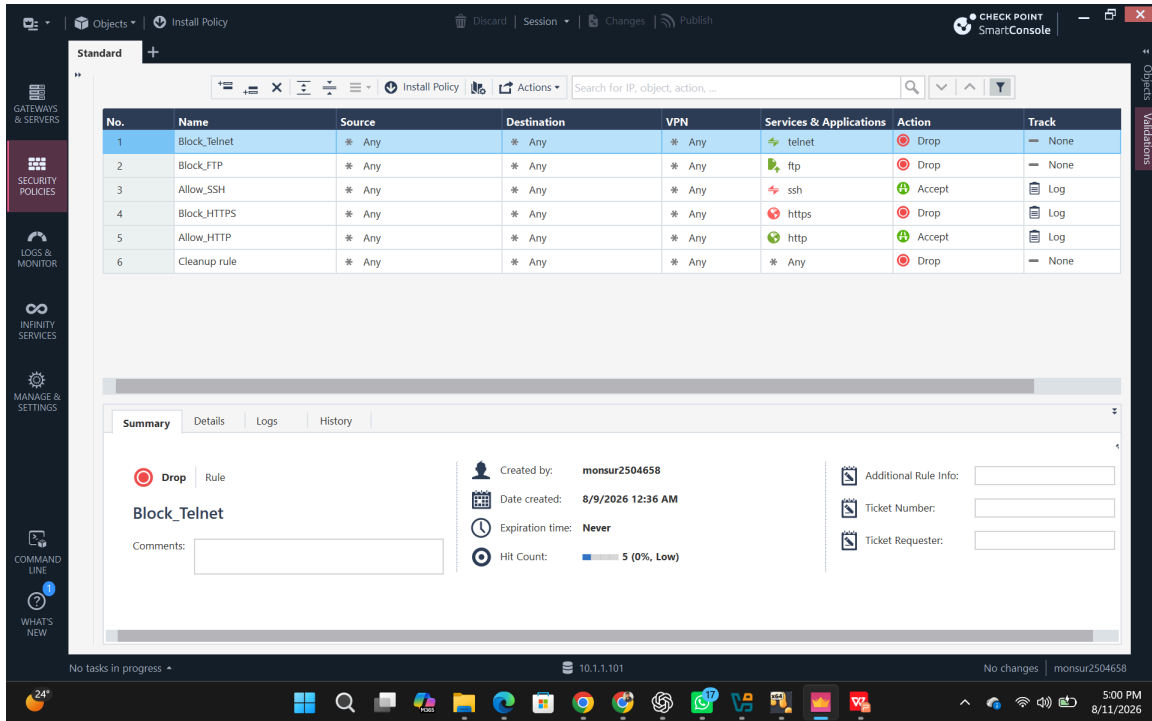


Figure 9. Firewall Policy Configuration

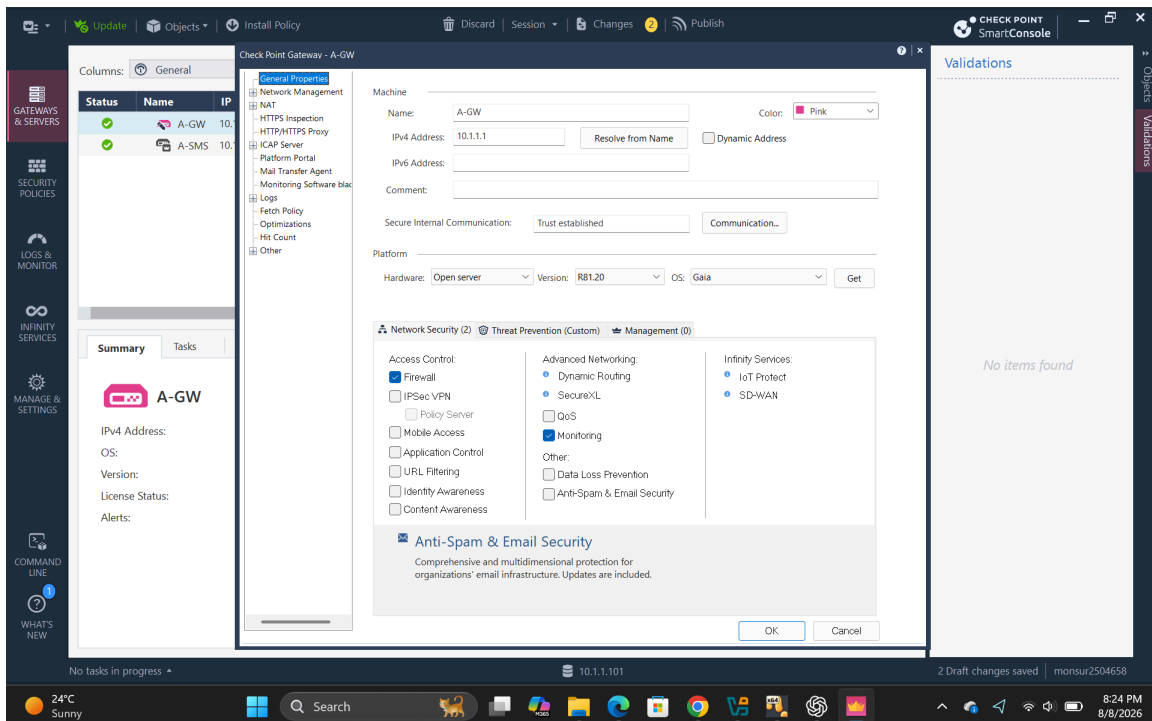


Figure 10. A-GW gateway Configuration

8. Policy Installation

Policy installation compiles the configured rules and pushes them from the management server to the gateway. Successful installation confirms that the gateway accepted the policy and is actively enforcing the configured access control rules [1]. The access control policy was installed successfully on the Security Gateway.

The screenshot shows the Check Point SmartConsole interface. The main window displays a table of rules under the 'Standard' policy. The 'Recent Tasks' pop-up window shows two successful installation events.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Block_Telnet	* Any	* Any	* Any	telnet	Drop	None
2	Block_FTP	* Any	* Any	* Any	ftp	Drop	None
3	Allow_SSH	* Any	* Any	* Any	ssh	Accept	Log
4	Block_HTTPS	* Any	* Any	* Any	https	Drop	Log
5	Allow_HTTP	* Any	* Any	* Any	http	Accept	Log
6	Cleanup rule	* Any	* Any	* Any	* Any	Drop	None

Recent Tasks

- Policy installation - Standard**
 - Installation succeeded on A-GW
 - 09-Aug-26 01:52:54 by monsur2504658
- Policy installation - Standard**
 - Installation succeeded on A-GW
 - 09-Aug-26 00:45:12 by monsur2504658

Task Details:

- Created by: monsur2504658
- Date created: 8/9/2026 12:36 AM
- Expiration time: Never
- Hit Count: 5 (0%, Low)

Additional Rule Info:

- Ticket Number:
- Ticket Requester:

Figure 11. Policy Installation

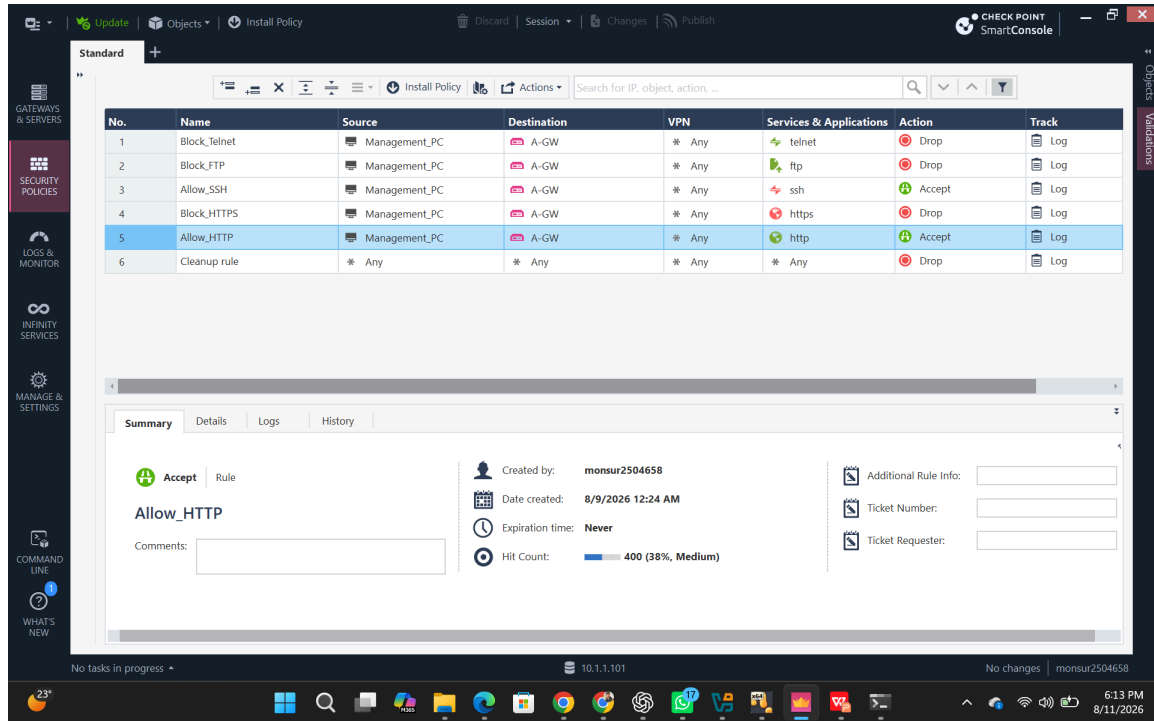


Figure 12. Role Configuration

9. Restricted User Group Configuration

A restricted user account and user group were created in Check Point SmartConsole to demonstrate identity-based access control. User groups allow administrators to apply security policies to multiple users collectively, improving policy management and reducing administrative complexity. The Restricted_Users group was configured to support controlled access permissions within the enterprise firewall environment.

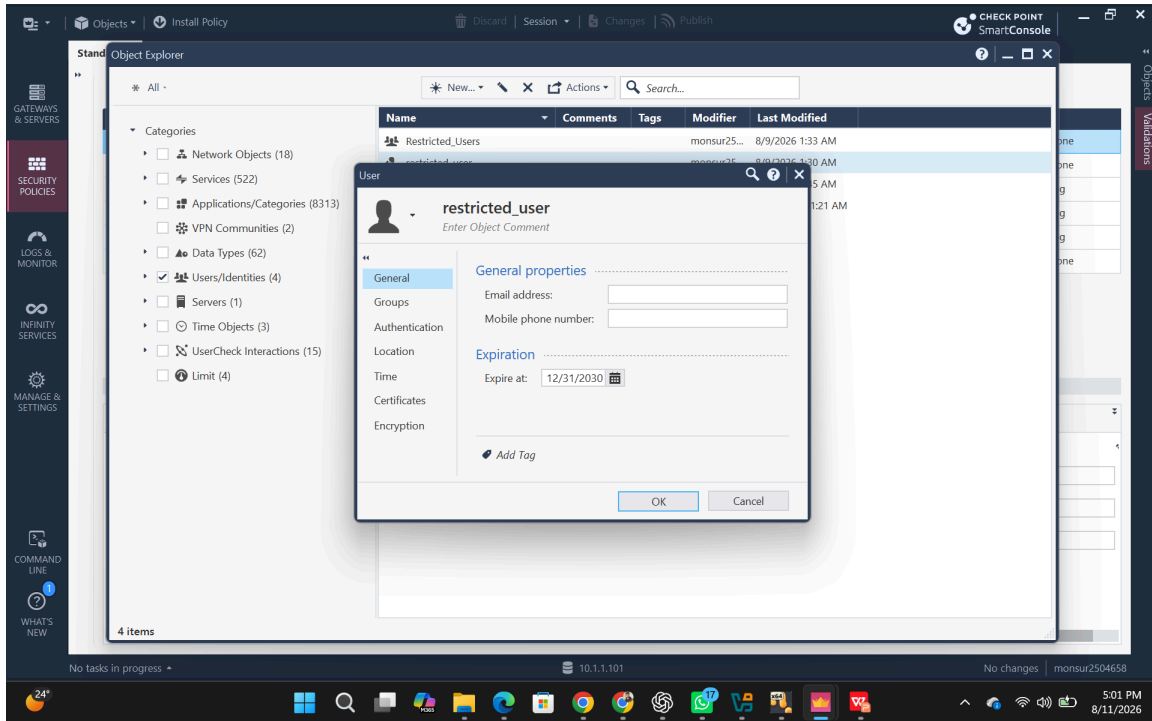


Figure 13. User Object Creation

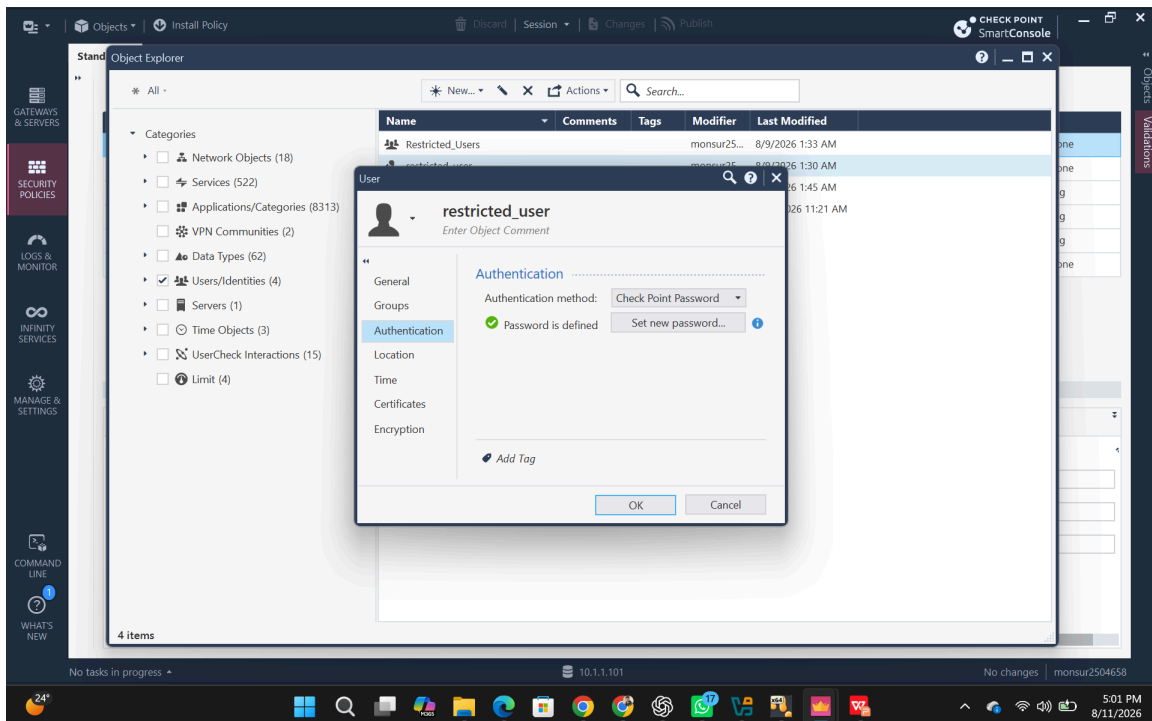


Figure 14. Restricted User Authentication

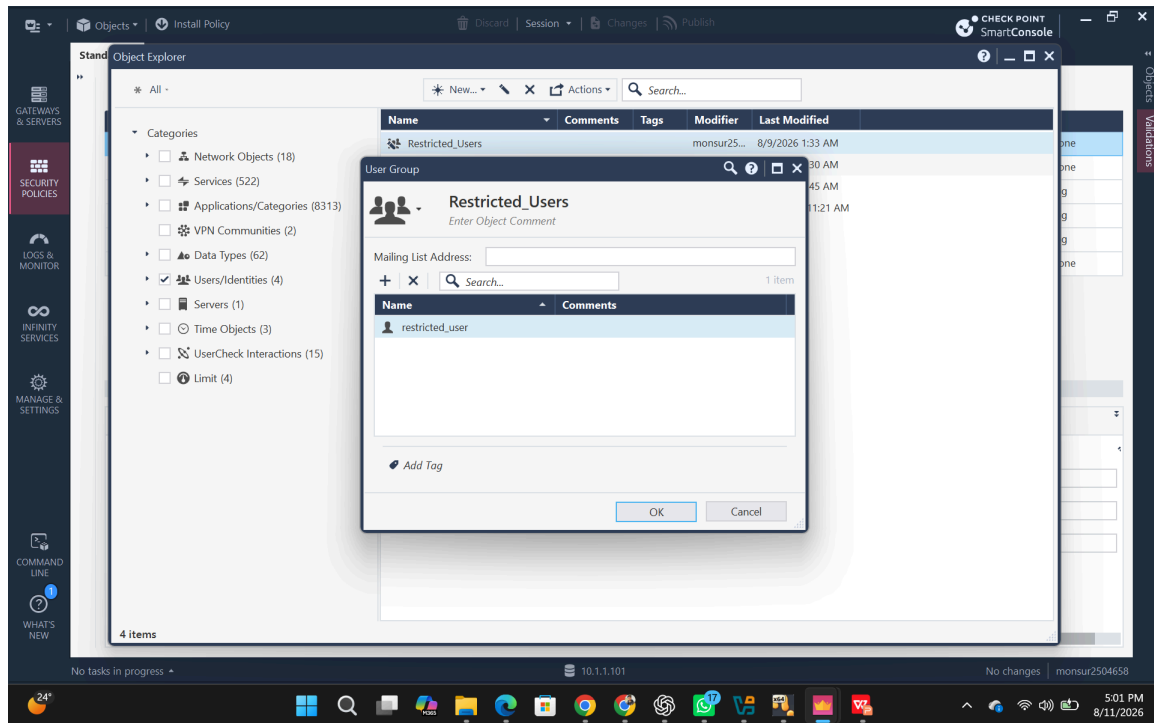


Figure 15. Restricted User Group Configuration

10. Traffic Verification

Traffic verification was performed from the Management_PC workstation by attempting to access the Security Gateway (A-GW) at IP address **10.1.1.1** using a web browser. The connection attempt generated HTTPS traffic that was processed by the Check Point Security Gateway. The browser returned an **ERR_CONNECTION_REFUSED** response, indicating that the requested service was unavailable or denied according to the configured security policy. This confirms that traffic was successfully generated and evaluated by the firewall before the corresponding events were examined in SmartConsole logs.

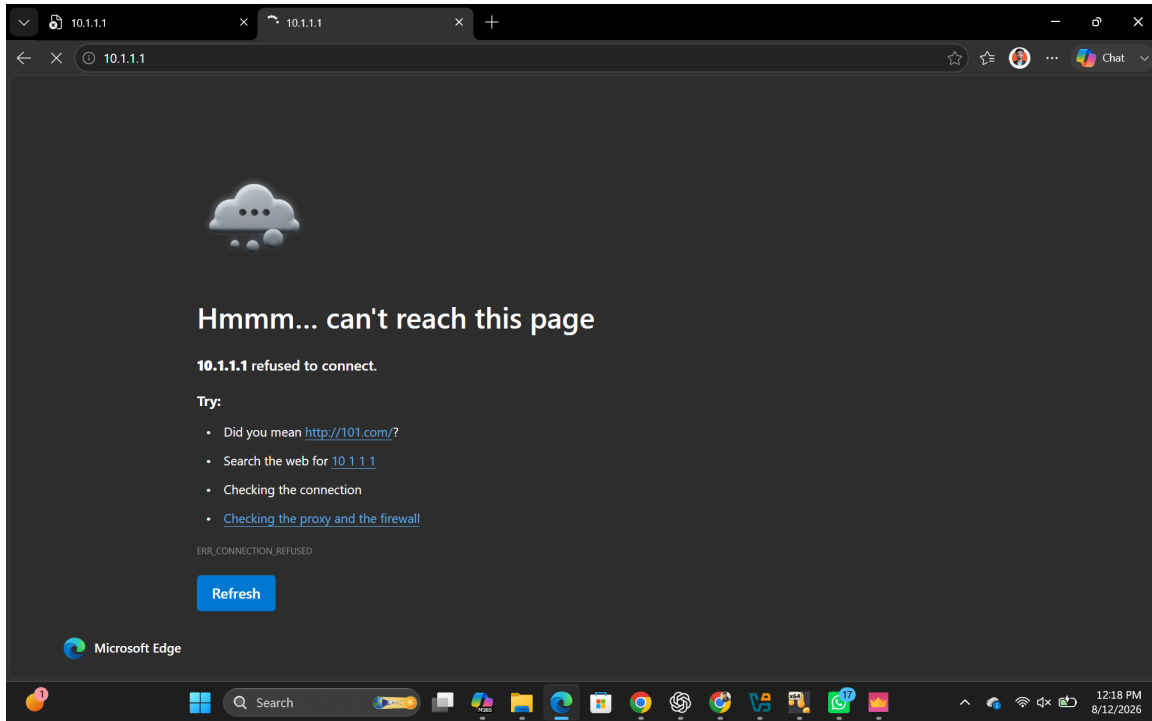


Figure 16. Traffic Verification Browser Connection Attempt

A browser-based connectivity test was performed from **Management_PC** by attempting to access the Security Gateway at **10.1.1.1**. The browser returned an **ERR_CONNECTION_REFUSED** response, indicating that the HTTPS connection attempt was denied or unavailable. This generated traffic that was subsequently verified through the SmartConsole log records shown in Figure 19.

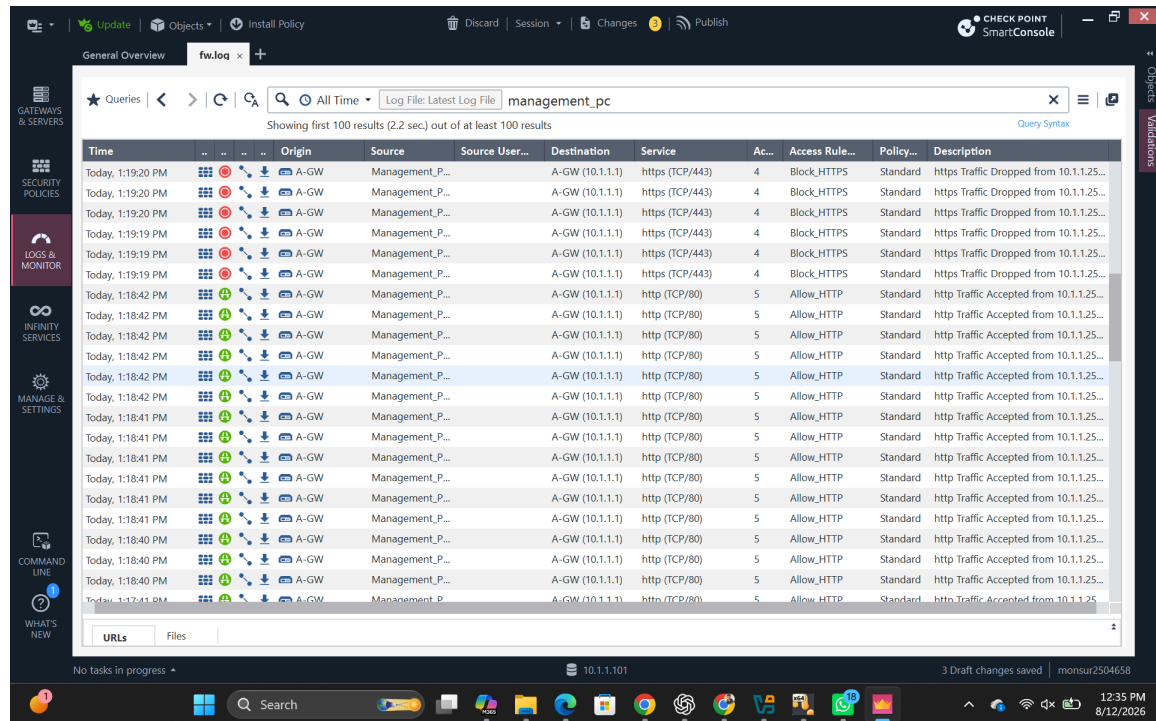


Figure 17. Traffic Verification Results in SmartConsole Logs

Figure 19 shows the results of traffic verification within the Check Point SmartConsole **Logs & Monitor** interface. Traffic generated from the **Management_PC** workstation to the **Security Gateway (A-GW)** at **10.1.1.1** was successfully processed by the firewall. The log entries demonstrate that **HTTP (TCP/80)** traffic was **accepted** under the **Allow_HTTP** rule, while **HTTPS (TCP/443)** traffic was **dropped** under the **Block_HTTPS** rule. The presence of both accepted and blocked events confirms that the installed firewall policy was correctly enforced and that SmartConsole successfully monitored and recorded network traffic according to the configured security rules.

11. Log Monitoring

Accepted and dropped log entries provide evidence that the firewall policy is functioning correctly. Log analysis supports security monitoring, troubleshooting, compliance verification, and forensic investigation by recording source, destination, service, rule, and action information [3], [5]. Firewall logs were reviewed to confirm accepted and dropped traffic events.

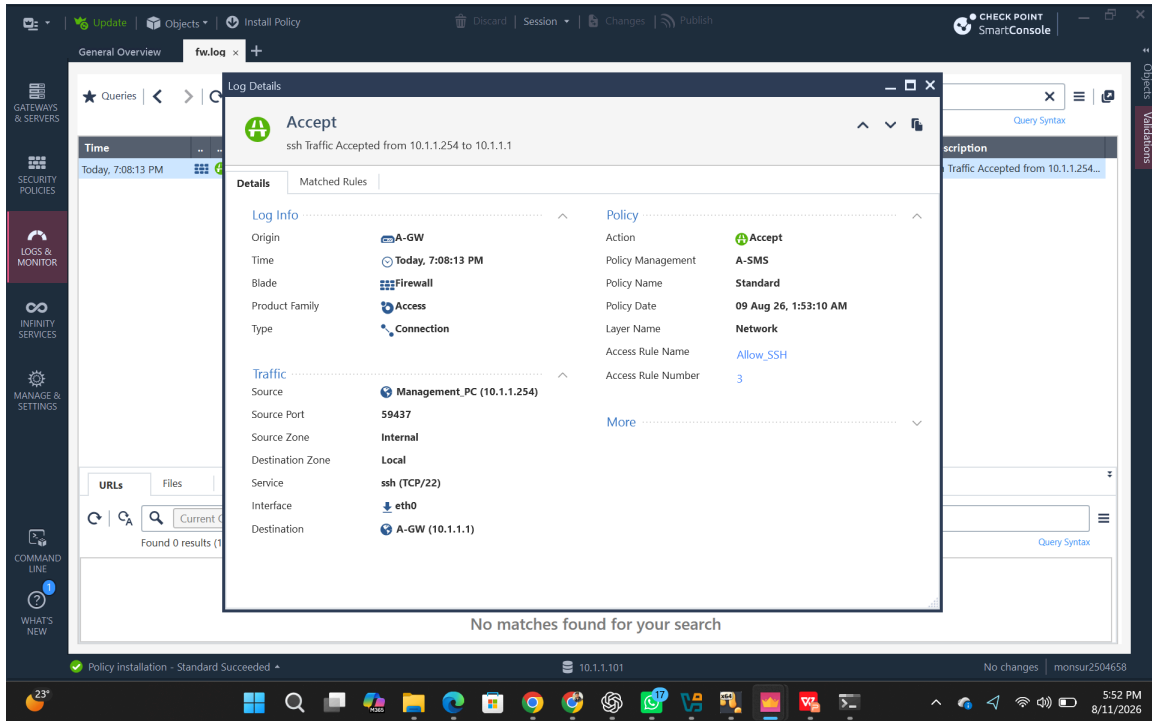


Figure 18. Log Details Accept

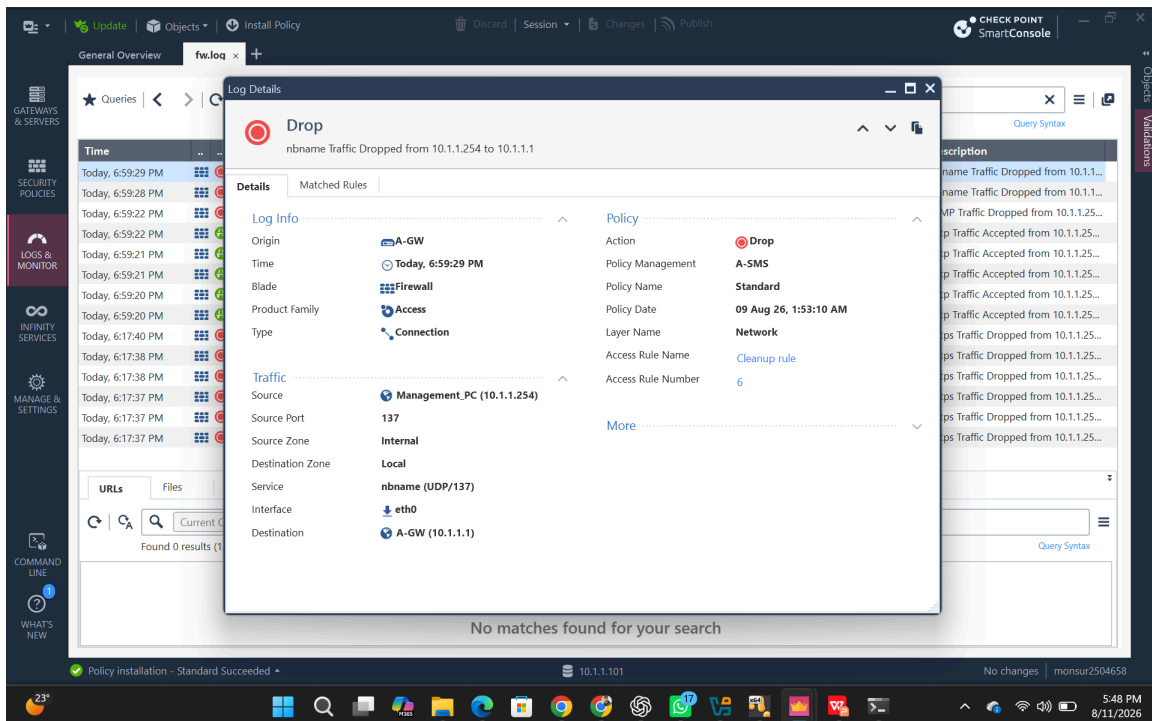


Figure 19. Log Details Drop

11. Evaluation

The implemented policy successfully permitted authorised HTTP and SSH traffic while denying insecure Telnet and FTP communications. The experiment demonstrated the effectiveness of Check Point SmartConsole in enforcing centralised access control policies. However, the lab environment was limited to a small simulated network and did not include advanced security blades such as IPS, Anti-Bot, or Threat Prevention. Future work could integrate these security features and perform penetration testing to evaluate firewall resilience under realistic attack conditions.

12. Conclusion

The practical implementation successfully demonstrated enterprise firewall administration using Check Point SmartConsole. Network segmentation, gateway verification, object configuration, policy deployment, traffic validation, and log analysis confirmed that authorised traffic was permitted while unauthorised traffic was blocked. These activities reflect core enterprise network security practices and support secure policy enforcement within organisational environments [1]–[5].

Video Link: [Monsur-2504658.mp4](#)

References

- [1] Check Point Software Technologies, *Check Point SmartConsole Administration Guide*, 2025.
- [2] Check Point Software Technologies, *Security Gateway Administration Guide*, 2025.
- [3] NIST, *Guidelines on Firewalls and Firewall Policy*, NIST SP 800-41 Rev.1.
- [4] W. Stallings, *Network Security Essentials: Applications and Standards*, 7th ed., Pearson, 2023.
- [5] ISO/IEC 27001:2022, *Information Security Management Systems Requirements*.
- [6] Cisco Systems, *Enterprise Network Segmentation Best Practices*, 2024.