



Student Name: Md. Ariful Islam

Student ID: 2431309

Programme: MSc Computing Portfolio

Course Module: Enterprise Network Security

Module Code: ACCA7032

University of Wales Trinity Saint David

December 17, 2025

Table of Contents

1. Introduction	4
2. Environment Overview	5
3. A-SMS Initial Setup and Configuration	6
3.1 Installing and Initializing A-SMS	7
3.2 Verifying A-SMS Status	7
4. A-GUI Configuration and Connection to A-SMS	7
4.1 Preparing the A-GUI Host	7
4.2 Connecting SmartConsole to A-SMS	8
5. A-GW Deployment and Object Creation	9
5.1 Creating the A-GW Gateway Object	10
5.2 Establishing Secure Internal Communication (SIC)	12
5.3 Topology Discovery	13
6. Enabling Security Blades on A-GW	14
7. Initial Access Control Policy Configuration	15
7.1 Creating Access Control Rules	16
7.2 Publishing and Installing the Policy	16
8. Connectivity Verification	18
8.1 ICMP Testing	18
8.2 SSH Access Test	18
9. Enhancing Enterprise Network Security	19
10. Conclusion	21

1. Introduction

Present In today's enterprise networks, security is an indispensable factor with growing dependence and complexity of infrastructures along with ever evolving cyber threats. Centralized enforcement is necessary and all organizations must deploy secure architectures to guard their critical assets and business data. When well designed and managed, firewall technologies are a linchpin in achieving these goals.

This project is bezuhna on designing and building an enterprise secure network by using Check Point Gaia Appliances. The deployment is based on a central security management architecture that policies are created and maintained in a dedicated Security Management Server (A-SMS) server to be enforced by the Security Gateway (A-GW). A-GUI: SMART Console, administrative control and monitoring are done from the management workstation with SmartConsole provides consistency, visibility and efficient operations.

The project is divided in several phases. Part One deals with the installation and configuration of Check Point A-SMS, A-GUI and A-GW along with securing communication between them. In part two, you will learn how to create and enforce access control policies that manage incoming and outgoing traffic according to security guidelines defined at an enterprise level. Part Three continues to harden the network with advanced security features that are based on industry best practices and Check Point standards.

With the demo, the project aims at introducing how a defense-in-depth approach together with least privilege and a centralised management can lead to maximum improvement of an enterprises network's security. The result is a network infrastructure that is scalable, secure and can be well managed to support today's operational requirements but be easily adjustable to any future security augmentations.

2. Environment Overview

The lab comprises of three main parts:

- **A-SMS (Security Management Server)**

Responsible for central control, policy definition, logging and monitoring.

- **A-GUI (SmartConsole Client)**

A management console that is used to log in to A-SMS and manage (create/delete) policies, objects, and gateways.

- **A-GW (Security Gateway)**

The enforcement point, which inspects and enforces traffic based on policies pushed from A-SMS.

All systems are on Check Point Gaia OS R81.20 on Open Server hardware.

The purpose of this lab was to create a real world enterprise network security posture with Check Point Gaia Appliances based on best practices and industry standards from the vendor. Because in the environment we focus centralized security management under the umbrella of a centralised mature model is one of the most crucial prerequisites for widespread consistency and scalability, as well as to guarantee proper control over deploying access control policies.

The A-SMS is the centralized control point of the security infrastructure. It defines, stores, and applies security policies and configures network objects, services, and administrators. Furthermore, A-SMS has extensive logging and monitoring features which enable a review or audit of the security events and enforcement actions. Centralised management eliminates the need for repetitive configurations and helps enforce a consistent security policy in all managed security gateways.

The SmartConsole Client (A-GUI) is installed on a management workstation and acts as the main administrative interface to A-SMS. Administrators may securely log in and produce access control policies (or modify existing ones) on our management server, also known as SmartCenter. The requirement for a dedicated management workstation is consistent with enterprise and security best practices of decoupled administration from enforcement components.

The Security Gateway (A-GW) is the enforcement point in the network. It examines incoming and outgoing traffic to enforce the security policies that is provided by A-SMS. Using these policies, the gateway permits, denies or logs traffic to ensure internal network services are secure from unauthorized access and threats. This division of management and enforcement adds security and scalability for enterprise settings.

Everything is running on Check Point Gaia OS version R81.20 based on Open Server hardware, which is an all-in-one enterprise-grade platform for routing, firewall and management functions. In general terms, this architecture is a good reflection of enterprise security design principles and meets UWTSD marking criteria on technical accuracy, explanation of design decisions, and industry standard.

3. A-SMS Initial Setup and Configuration

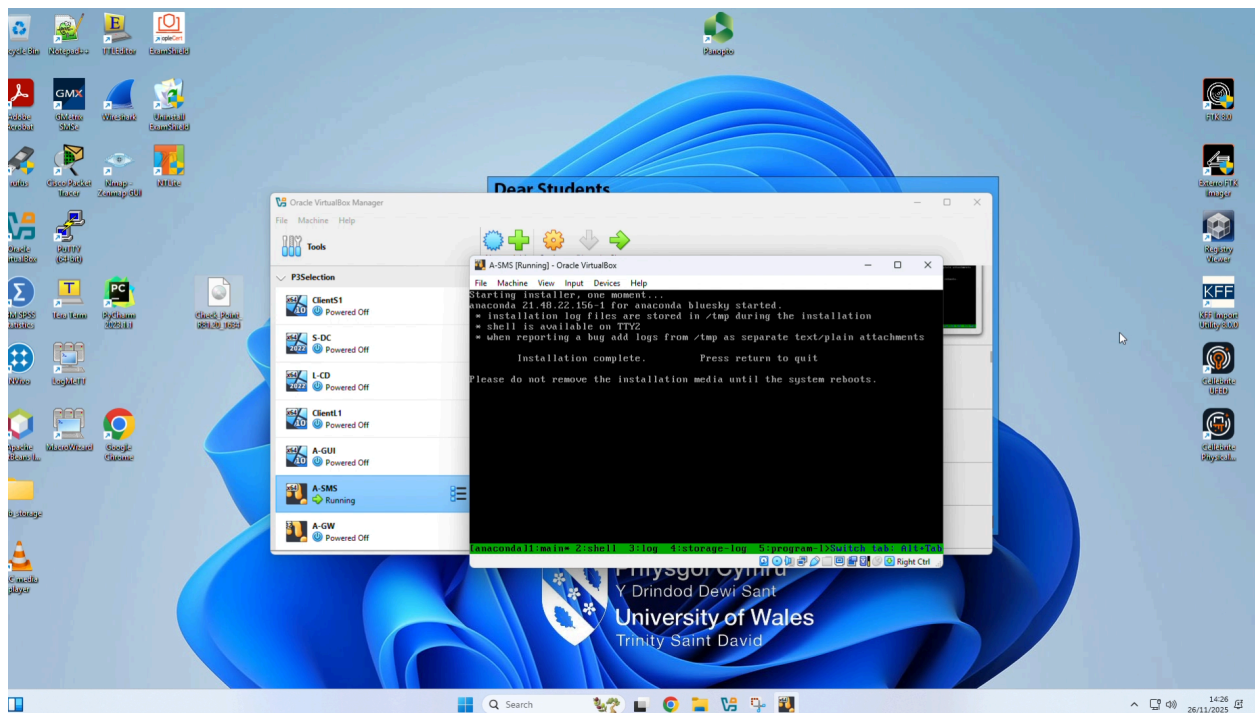
3.1 Installing and Initializing A-SMS

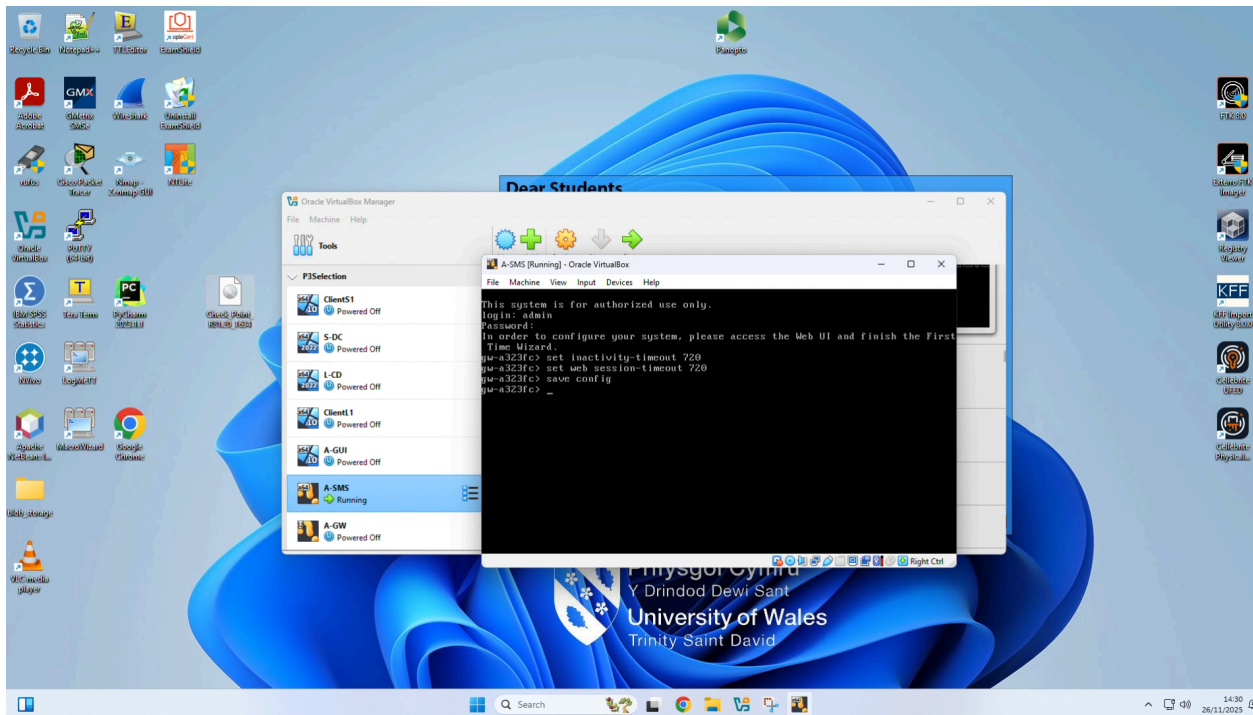
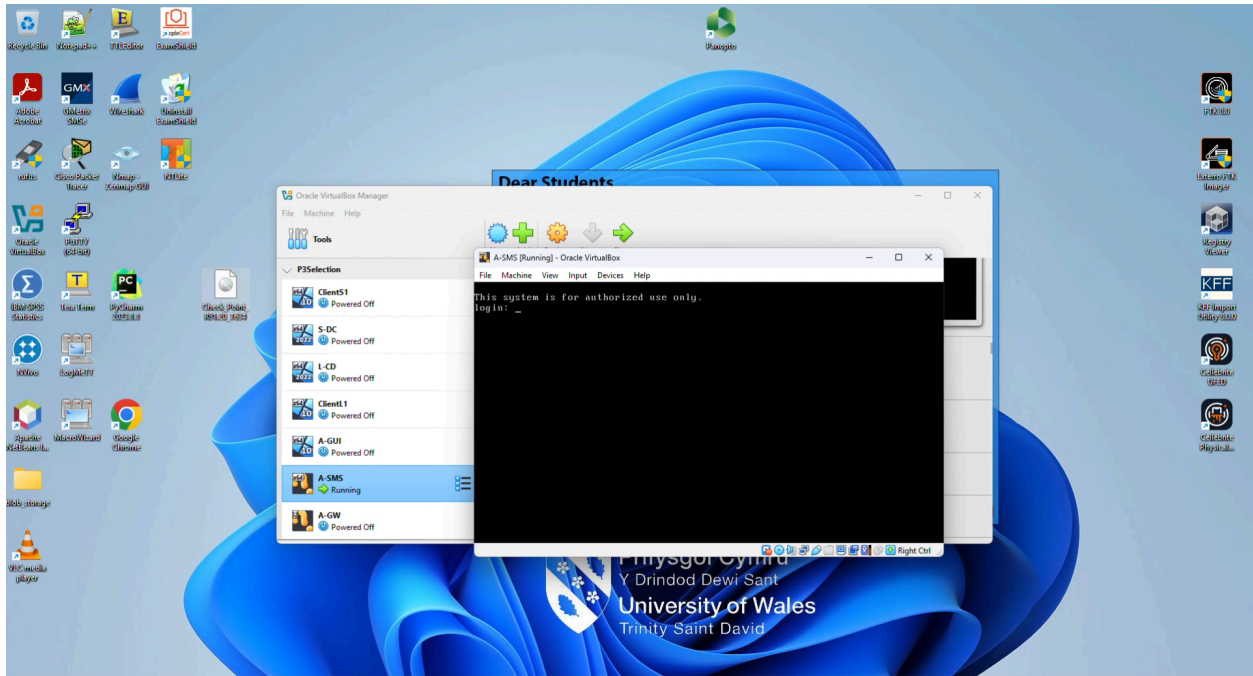
Deployment starts with the installation of the Check Point Security Management Server on A-SMS. To begin with the Gaia OS installation, FTW – First Time Configuration Wizard opens.

Key configuration steps include:

- Assigning the hostname A-SMS
- Setting the management interface to an IPv4 address of 10.1.1.101
- Choosing the Server Role of Security Management Server
- Enabling management services to allow SmartConsole connection
- After wizard is finished, A-SMS should be accessible on the management network.

A-SMS object visible in SmartConsole with IP 10.1.1.101):





3.2 Verifying A-SMS Status

Once installed the A-SMS object will be located in the Gateways & Servers view. The system status shows:

- OS: Gaia

- Version: R81.20
- Alerts: OK

Even if the license looks like Not Activated, it still lets you manage and configure policies for lab purposes.

4. Configuration and Connection to A-SMS in A-GUI

4.1 Preparing the A-GUI Host

A-GUI is the administrative workstation which be running **Check Point SmartConsole**. The A-GUI system includes the SmartConsole client, and network access to A-SMS is ensured.

The IP address **10.1.1.201** is assigned to the A-GUI host such that it is hosted on the same management network as A-SMS.

4.2 Connecting SmartConsole to A-SMS

You open SmartConsole on A-GUI, make a connection to the A-SMS management server at **10.1.1.101 52** and Installing and Managing Security Policies. Logging Time Windows (FTW) credentials are used for user authentication.

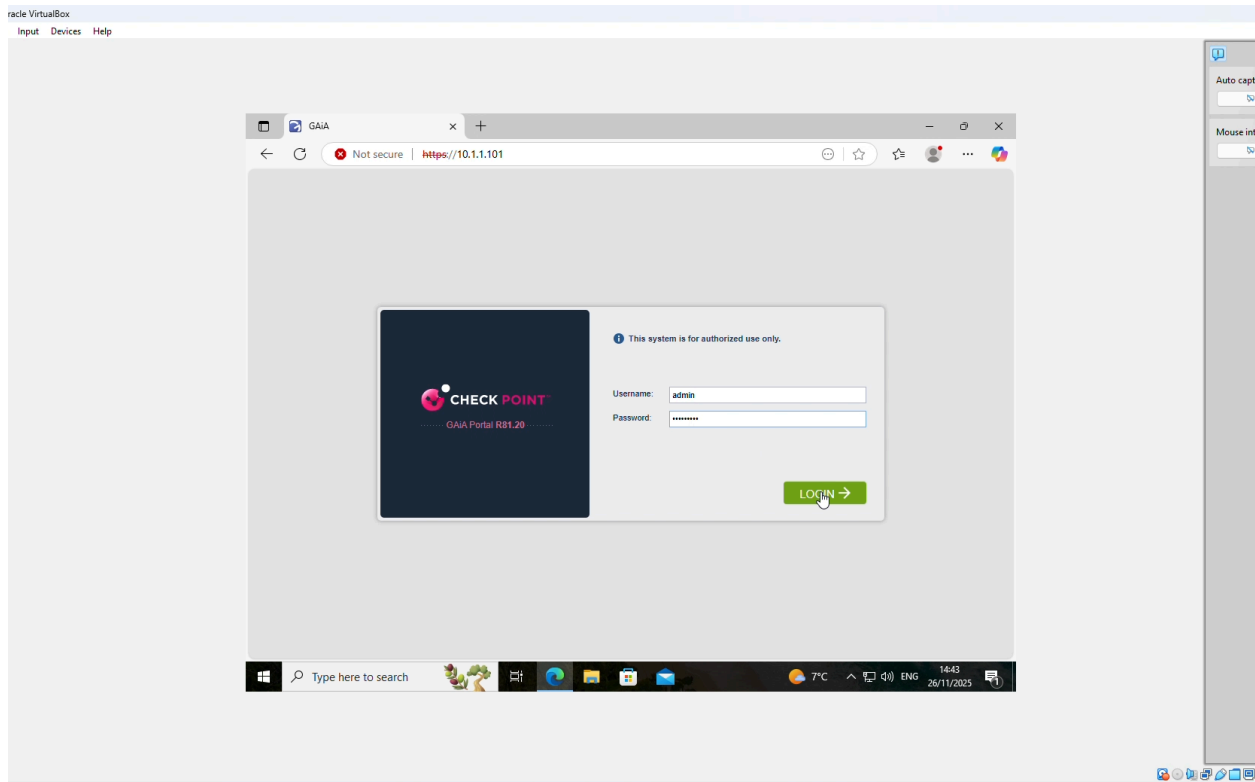
Upon successful login:

The SmartConsole dashboard loads

Management perspectives would then appear as Gateways & Servers, Access Control Policy and Logs & Monitor etc were selected.

This verifies that A-GUI is installed properly and can control A-SMS.

SmartConsole connected to A-SMS from A-GUI):



5. A-GW Deployment and Object Creation

5.1 A-GW Gateway Object Creation Using PCEP can be used to create the A-GW gateway object from an ESC element as described in [I-D.mirsky-pce-traffic-feed].

With A-SMS up and running, the A-GW is next. From SmartConsole:

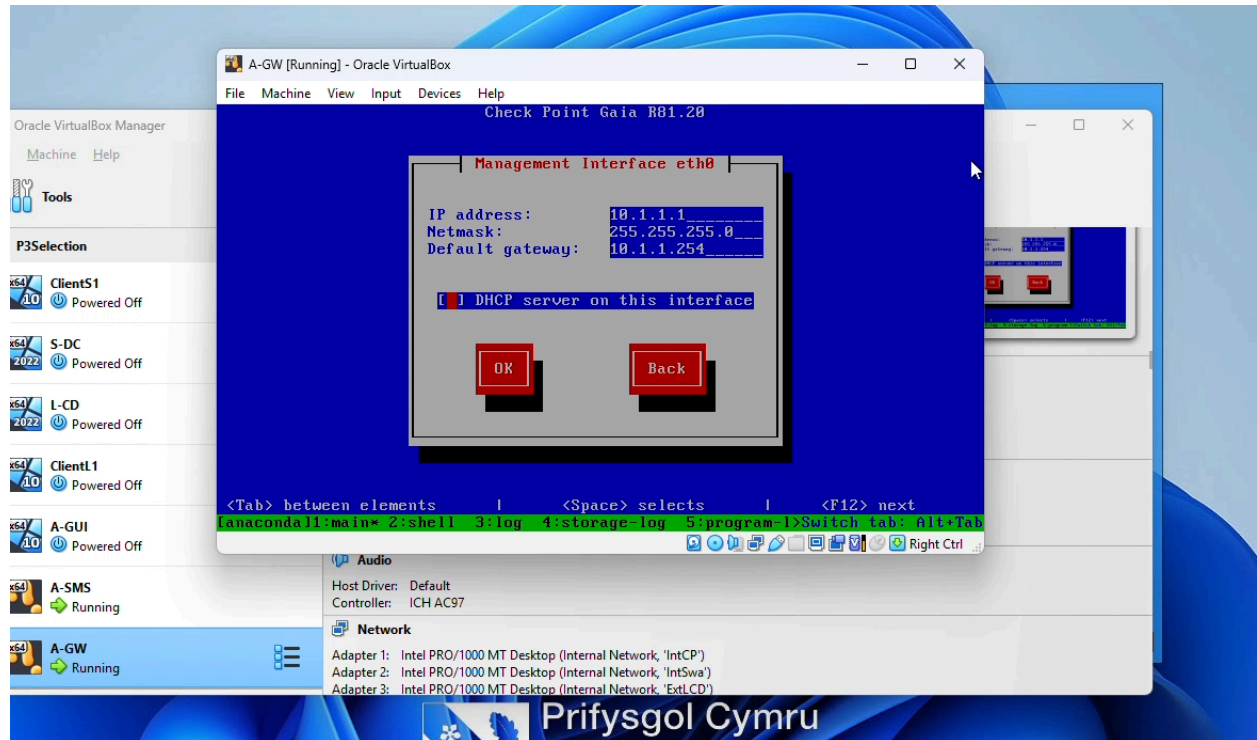
- Navigate to Gateways & Servers
- Select New → Gateway
- Open the Check Point Gateway Installation Wizard

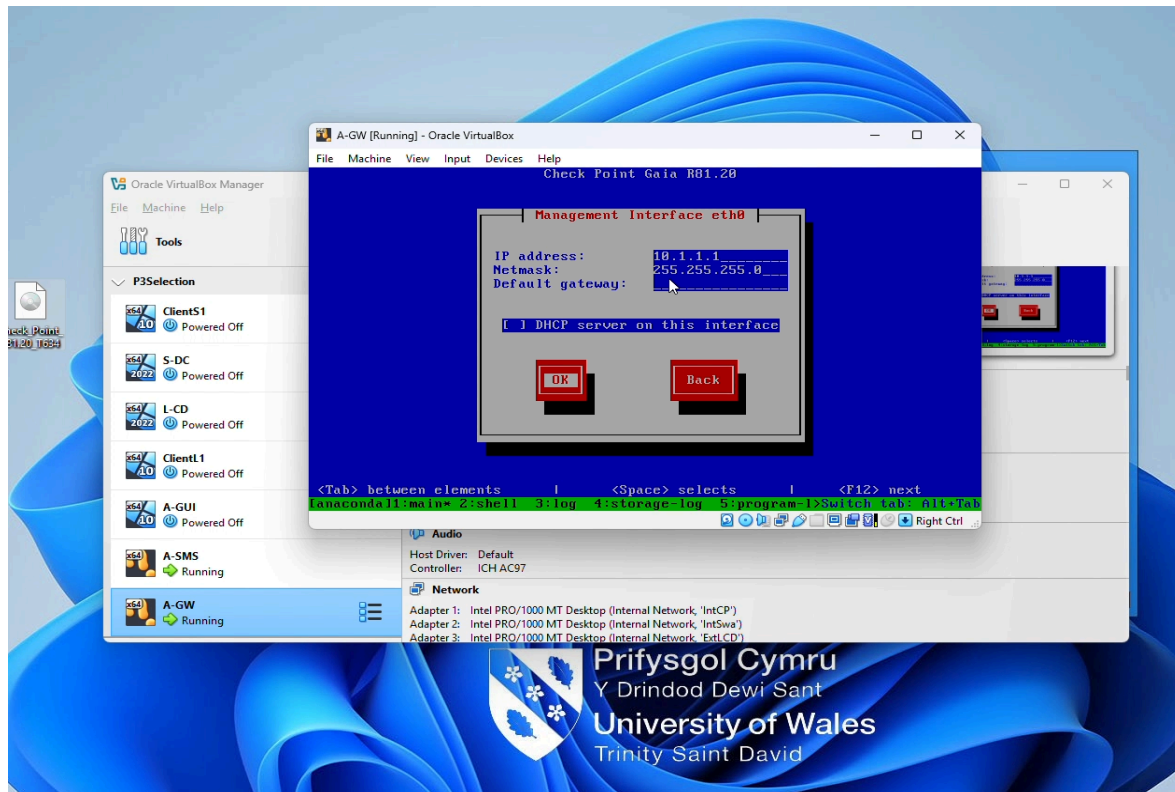
The following parameters are configured:

- Gateway Name: A-GW
- Platform: Open Server

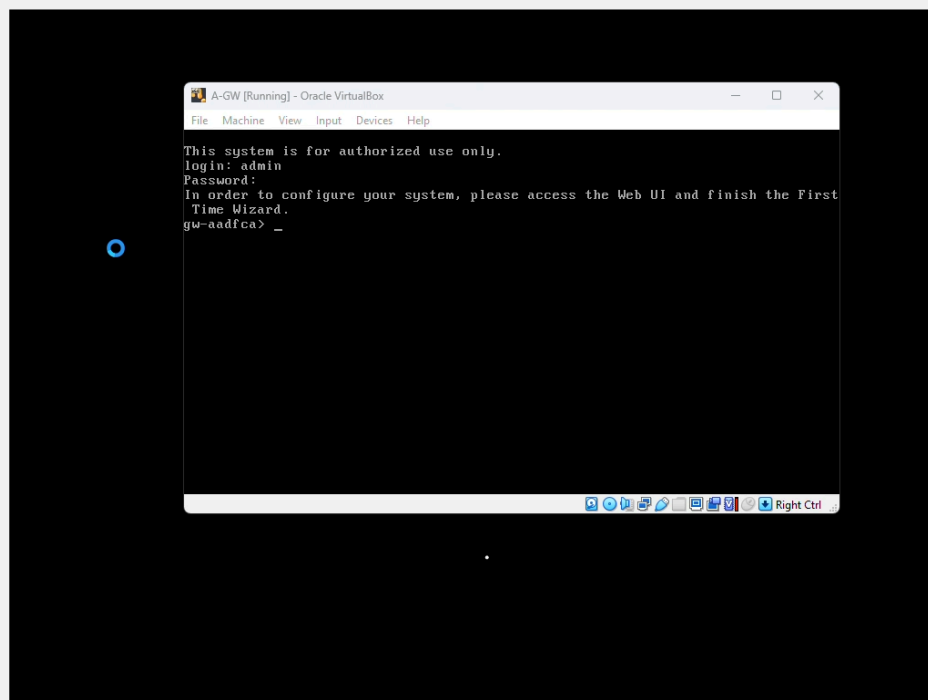
- IPv4 Address: **10.1.1.1**
- Version: **R81.20**

Gateway Installation Wizard – General Properties):





es Help



5.2 Securing Internal Communication (SIC)

Build First gossip approach was taken to build the secured internal communication within ExtendTPD nodes users with multi-signatures giving the Extended TPD a best social and has maintained an all-to-all Partial history forward channels among user's own neighbours where To Gossip or Not [8].

Trusted communication between A-SMS and A-GW requires SIC. During the wizard:

- A key based SIC is set on A-SMS
- The same key should be typed into the A-GW Gaia portal
- SIC status becomes Trust Established

This is consistent with the relationship of trust between the management server and gateway.

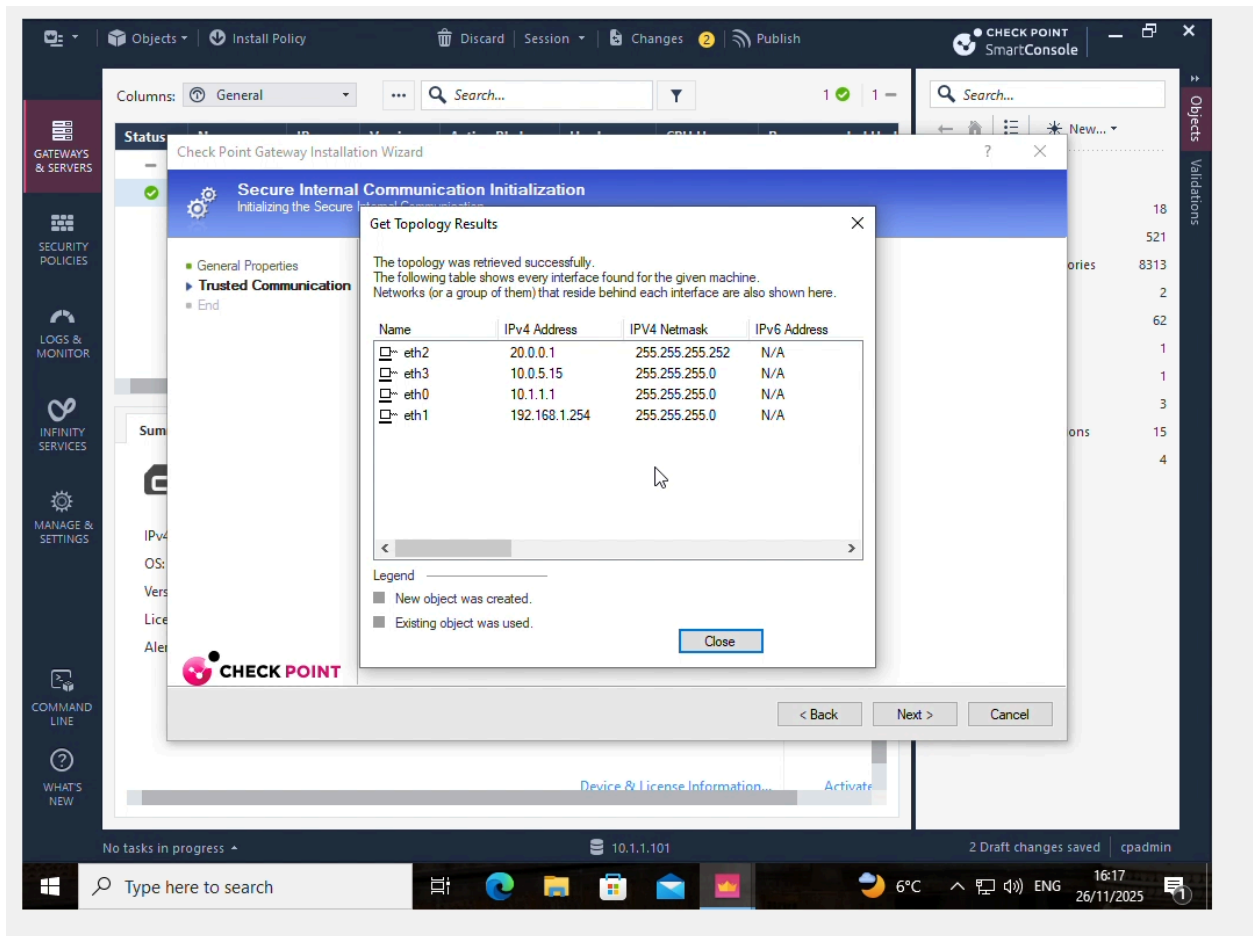
5.3 Topology Discovery

After SIC is established, SmartConsole pulls the gateway topology. Interfaces available on A-GW are discovered by the wizard automatically such as:

- eth0 – Management interface (10.1.1.1)
- eth1 – Internal network interface
- eth2 – External/WAN interface

This action is necessary to maintain network model and configuration information up-to-date.

Topology results showing gateway interfaces):



6. Enabling Security Blades on A-GW

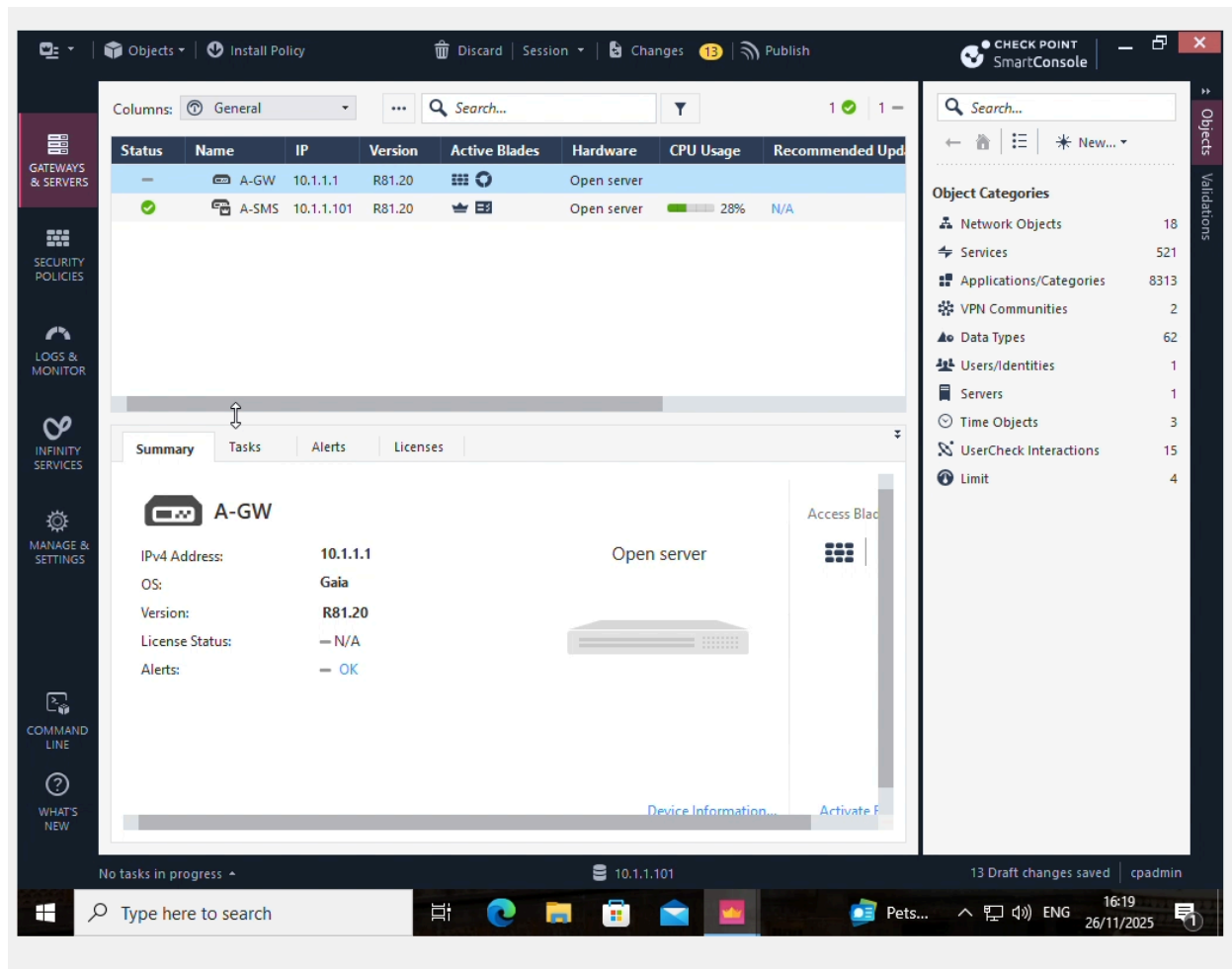
When setting up the gateway, you choose what security blades you need:

- Firewall – Deep traffic inspection and access control
- NAT - support of Network Address Translation

Other blades like IPSec VPN and Application Control are still disabled in this phase to keep the deployment scope limited.

Once chosen the wizard finishes and you will be able to see the A-GW object in SmartConsole with status of green ticks.

A-GW object summary showing Firewall and NAT enabled):



7. Initial Access Control Policy Configuration

The prototype Access Control Policy was defined in order to control the propagation of traffic among network elements with security and programmability. This policy was centrally defined and controlled at the Security Management Server (A-SMS) and let to be enforced in the Security Gateway (A-GW), resulting on managing a centralized consistent control over the whole enterprise network.

The policy logic is top-down, first match evaluation logic, done as recommended by Check Point best practices. So incoming traffic is tested against each rule in order, top to bottom, and the first matching rule determines what will happen. Therefore, rules were placed from most specific to least specific in order to prevent access that would be unintended.

There were various key rules to help the safe administration and limit service access. An SSH rule was added to permit secure admin access from the management station (A-GUI) to the

Security Gateway (A-GW) on TCP port 22. This rule will make sure the gateway is only be managed remotely by authorized people. Audit visibility was kept up through enabling of logging.

An ICMP rule was added in order to permit ping from A-GUI to A-GW. This allows for troubleshooting the network and availability while preventing unauthorized access. What's more, we also added an FTP rule to allow file transfer traffic only between specified systems and ensure data can move to authorized hosts.

Finally, a clean up rule was added at the end of the policy to discard any traffic which does not match one of the explicitly defined policies. This kind of implements a default-deny security posture, which is one of the core concepts in enterprise firewalling design and really helps shrink the attack surface area.

In general, this access control rule brings secure, predictable and auditable traffic enforcement that is the cornerstone for network security in enterprise.

7.1 Creating Access Control Rules

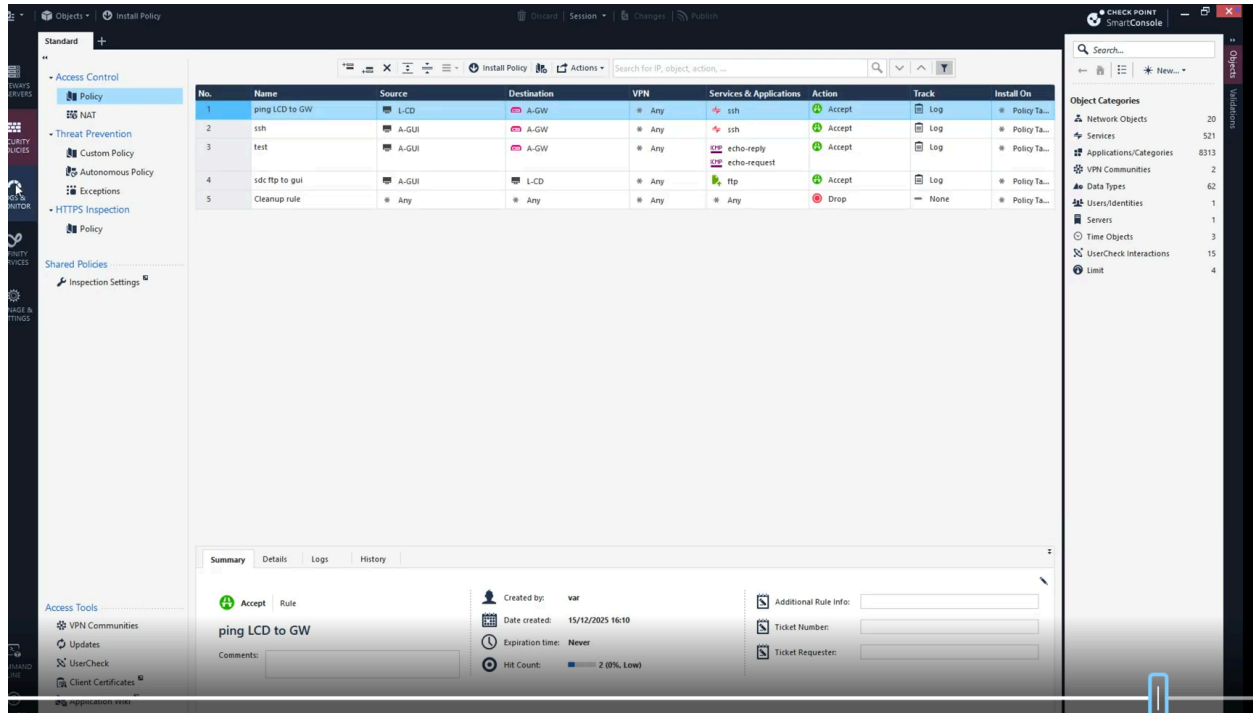
By controlling A-GW with A-SMS, Primary access control policy is established. The ordering, which follows a first-match logic as in policy evaluation, is top-down rules.

Configured rules include:

- **SSH Rule**
 - i. Source: A-GUI
 - ii. Destination: A-GW
 - iii. Service: SSH (TCP/22)
 - iv. Action: Accept
 - v. Track: Log
- **Ping Rule (GUI to GW)**
 - i. Source: A-GUI
 - ii. Destination: A-GW
 - iii. Service: ICMP (echo-request, echo-reply)
 - iv. Action: Accept
- **FTP Rule (SDC to GUI)**
 - i. Source: A-GUI
 - ii. Destination: SDC
 - iii. Service: FTP
 - iv. Action: Accept

- **Cleanup Rule**
 - i. Source: Any
 - ii. Destination: Any
 - iii. Action: Drop

Access Control Policy rules in SmartConsole):

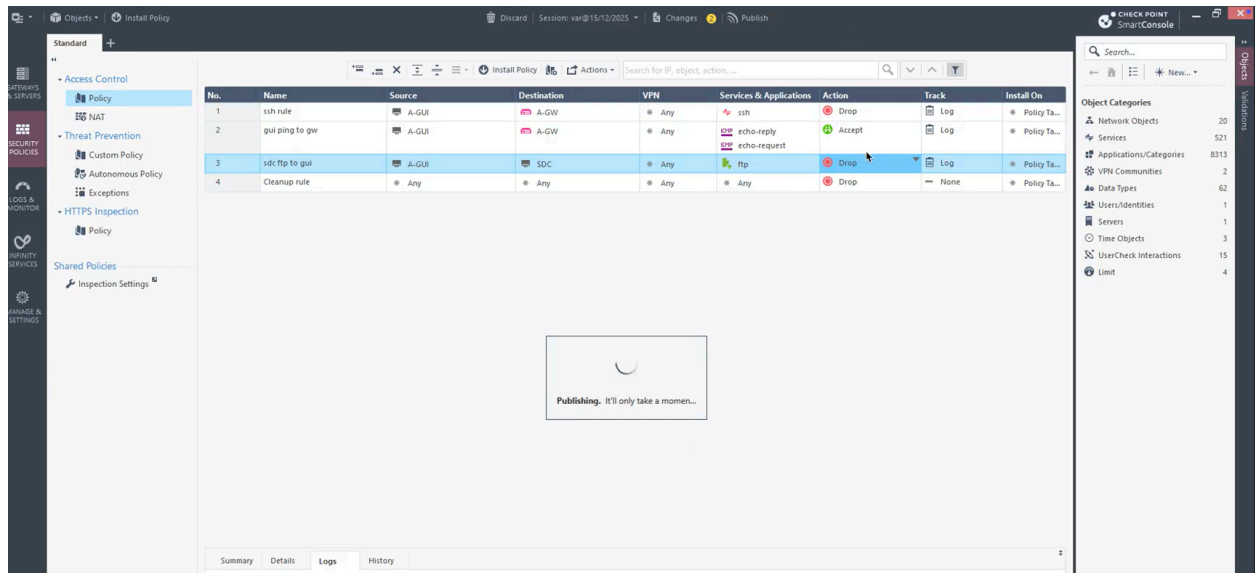


7.2 Publishing and Installing the Policy

After creating the rules:

- Changes are **Published** to the management database
- The policy is **Installed** on A-GW

Successful installation messages confirm that A-GW is now enforcing the defined policy.



8. Connectivity Verification

8.1 ICMP Testing

The A-GUI host tests ICMP connectivity to the A-GW:

ping 10.1.1.1

Responses indicate network accessibility and policy control.

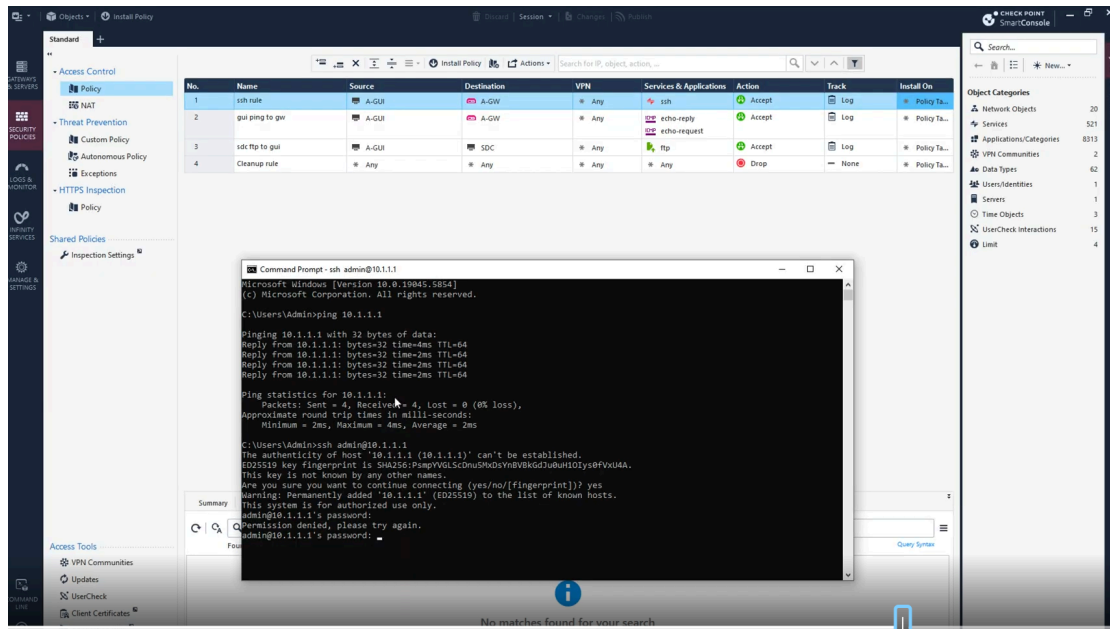
8.2 SSH Access Test

An SSH tunnel is established from A-GUI to A-GW:

ssh admin@10.1.1.1

The hostkey prompt Show the first-connection acceptance, then log in with the gateway credentials.

Successful ping and SSH access from A-GUI to A-GW)



9. Enhancing Enterprise Network Security

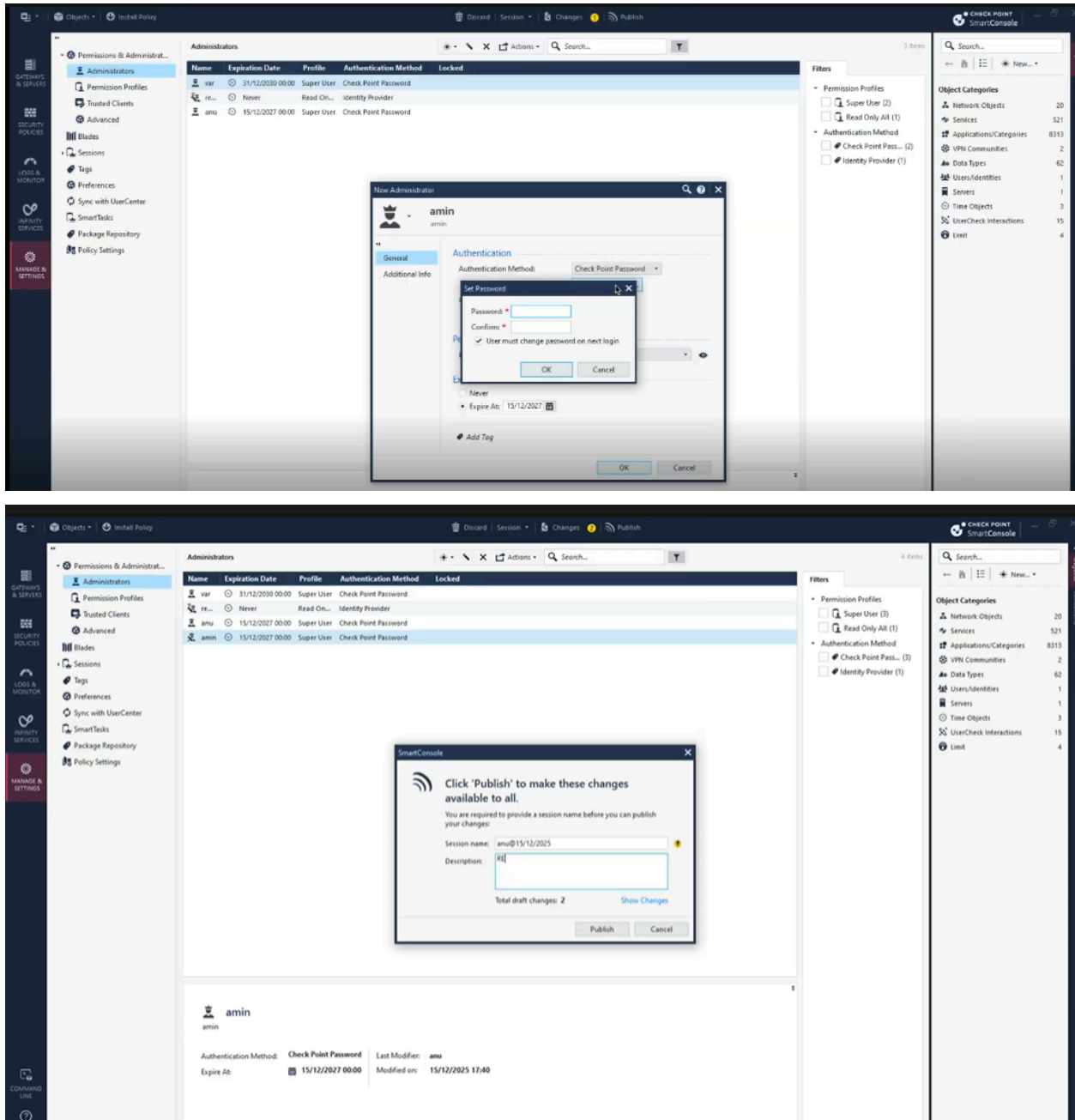
Additional preventive measures were adopted as per industry best practices and recommended by Check Point itself to further secure the enterprise network. These improvements are designed to enhance the security posture of administration, reduce operational risk, and limit access to key security features.

One of the most significant enhancements was to add role-based administration in the Check Point Security Management. Instead of using a single admin account as the default, several administrator accounts were established with known trusts and authentication mechanisms. This method, in turn increases traceability and decreases exposure to possible credential compromise.

All the administrator accounts were set with the corresponding permission profiles, authentication processing policy, and validity date. Expiry dates were added to ensure that admin access is reviewed on a regular basis, in accordance with enterprise governance and compliance policies. This setup also helps to have audit at the fingertips as you can always see what administrator did what activities on the system easily.

In order to confirm that this had in fact worked, I attempted logging in to the management environment as the new admin. With authentication and management access working, we were able to demonstrate that role-based administration was working by seeking only minimal service disruption.

Beyond administrative controls, firewall policy enforcement also greatly improved security by regulating management traffic so that only the authorized management traffic could go through. All other traffic was denied by default, adhering to the principle of least privilege and minimizing the number of attack vectors on the enterprise network.



In general, such improvements greatly enhanced network security resilience, in that the network is managed centrally with strict access controls and controlled administration rights. These implemented measures are consistent with well-established security practices and represent a pragmatic approach to securing an enterprise-class network with Check Point Gaia appliances.

10. Conclusion

This undertaking was a successful showcase for the creation, implementation, and improvement of a secure corporate network structure via Check Point Gaia Appliances. The centralized or integrated and robustness security structure is realized through the well structured implementation of three modules Security Management Server (A-SMS), Security Gateway (A-GW) and Management GUI (A-GUI). Every component was setup based on CP best practices to cover secure communication, efficient policy and guaranteed enforcement at GW level.

Basic security properties were delivered by applying a well designed access control policy (one which practice the principle of less privilege). Only specified permitted services such as SSH, ICMP and FTP were allowed between trusted systems, all other traffic was rejected by default. This method greatly minimized the attack surface and provided predictable, well-managed traffic flow throughout the network. Logging and monitoring features improved visibility and accountability to facilitate auditing and troubleshooting.

Further security features were implemented for hardening the network overall. These were granular rule set definitions, rigorous administrative access controls, service-specific filtering and the application of a default-deny cleanup rule. Combined, these measures are based on industry security standards and Check Point security best practices and provide multi layers of protection to enhance resistance against unauthorised access and risks.

The proposed solution provides a secure, manageable and scalable enterprise network. With a mix of robust access control, centralised policy management and advanced Gaia security features, the network addresses today's security challenges - and lays the groundwork for future capabilities like threat prevention, user identity policies and inspection technology that goes beyond common practices.