



**Module:** Enterprise Network Security

**Module Code:** ACCA7032

**Submitted to:**

Mr. Munyaradzi Murira

Associate Professor

University of wales trinity saint david

**Submitted By:**

MD IMRAN BISWAS

Student ID: 2436882

University Of Wales Trinity Saint David

**Submitted Date: 22-01-2026**

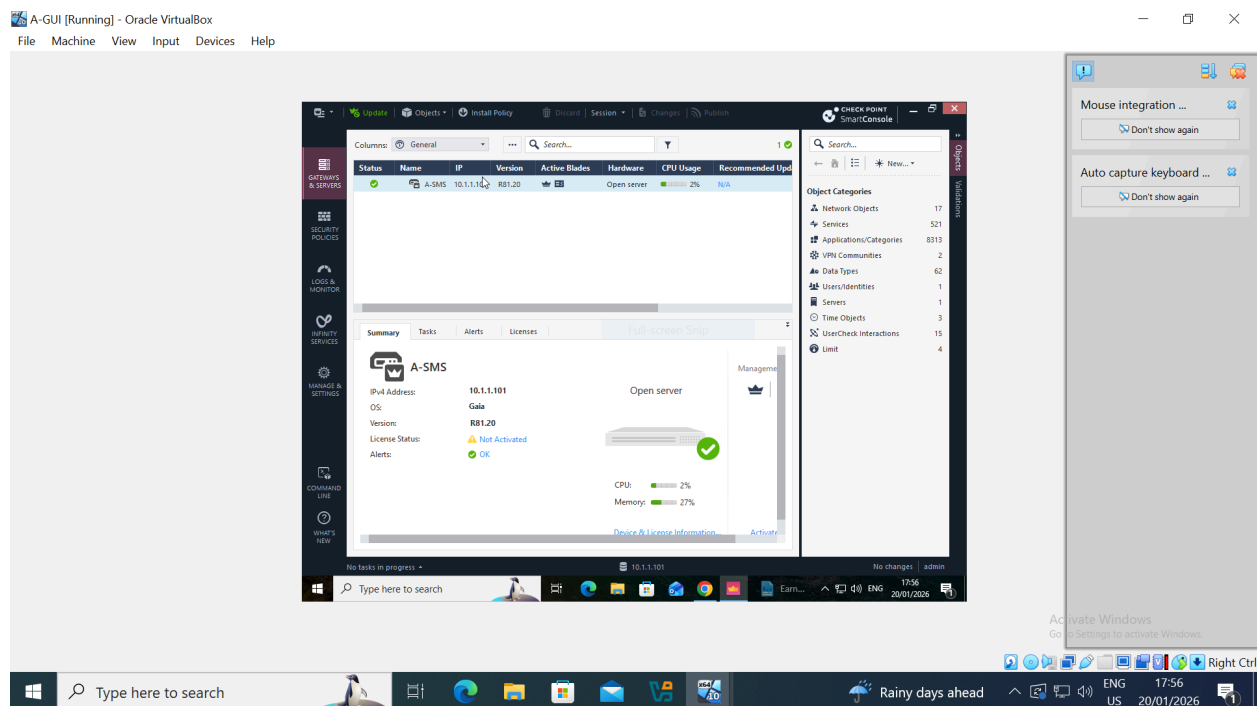
# Introduction

The primary goal of this lab is to design, deploy, and configure a secure network architecture by integrating a Security Management Server (A-SMS), Security Gateway (A-GW), and Management GUI (A-GUI) with an existing enterprise domain infrastructure. This lab focuses on implementing enterprise network security using Check Point GAiA appliances within a controlled lab environment.

The exercise expands upon company networks that have already been set up and shows how internal network protection may be achieved through centralized security administration and policy enforcement. This lab establishes secure communication between several network segments, such as the primary data center (S-DC) and the local data center (L-DC), while managing licenses, enforcing firewall restrictions, and verifying Secure Internal Communication (SIC).

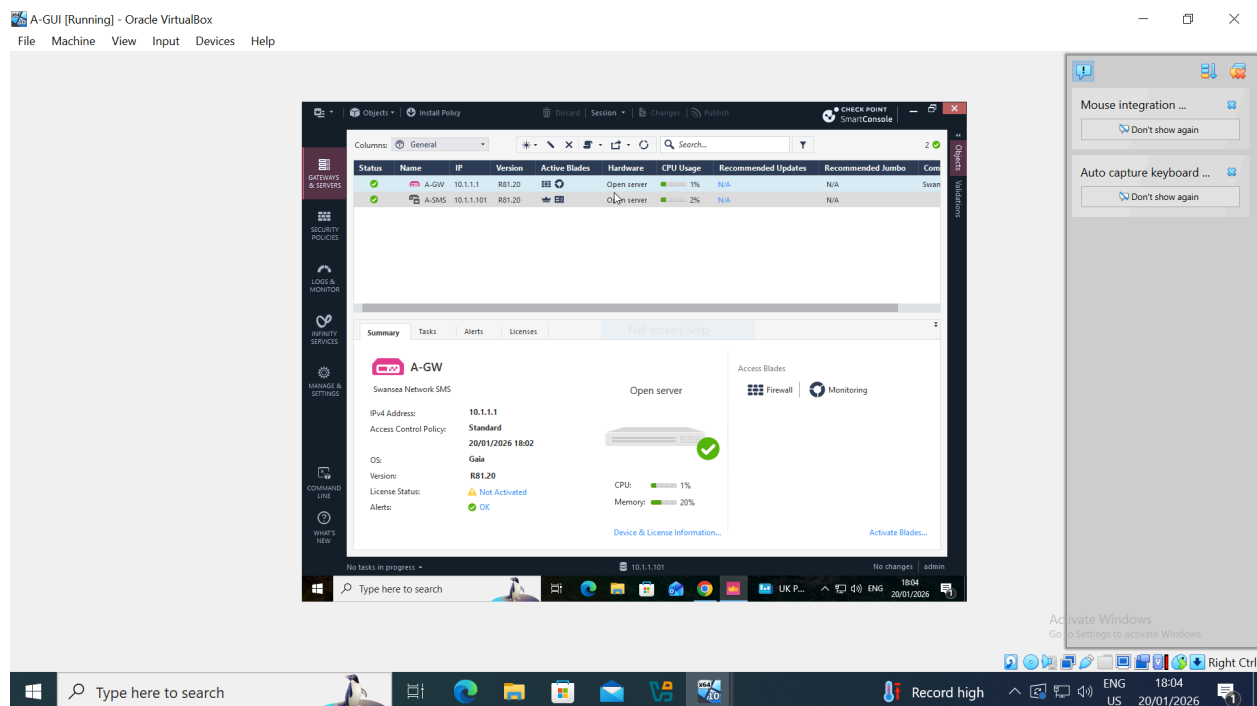
All things considered, this hands-on exercise offers practical experience in implementing enterprise-grade security solutions, comprehending real-world network segmentation, and implementing security rules to successfully secure organizational resources.

## Smart Console Setup



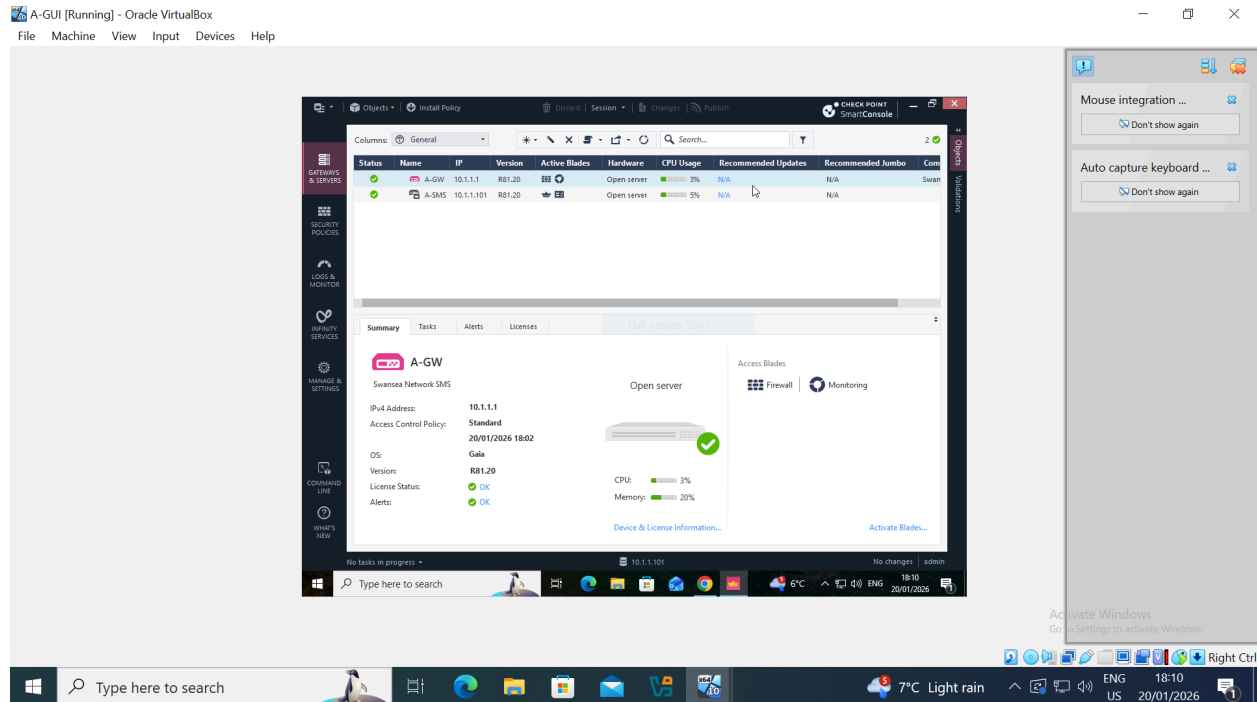
The A-GUI system has successfully installed and configured the Check Point SmartConsole. The SmartConsole interface displays and allows access to the Security Management Server (A-SMS), indicating effective connectivity and management integration. Check Point GAiA R81.20 is being used by the A-SMS; the system status indicates that it is operating normally and that there are no active alerts. This verifies that the management environment is properly configured and prepared for duties related to security management, monitoring, and policy configuration.

## Security Gateway (A-GW) Added Successfully



The Check Point Security Gateway (A-GW) was successfully added to the Security Management Server (A-SMS) following the completion of the SmartConsole setup. Now that the gateway is visible in the Gateways & Servers area, Secure Internal Communication (SIC) has been properly set up. The system status indicates normal operation with no current alerts, and the A-GW is operating on Check Point GAiA R81.20 with firewall and monitoring blades enabled. This attests to the gateway's preparedness for traffic enforcement and policy installation.

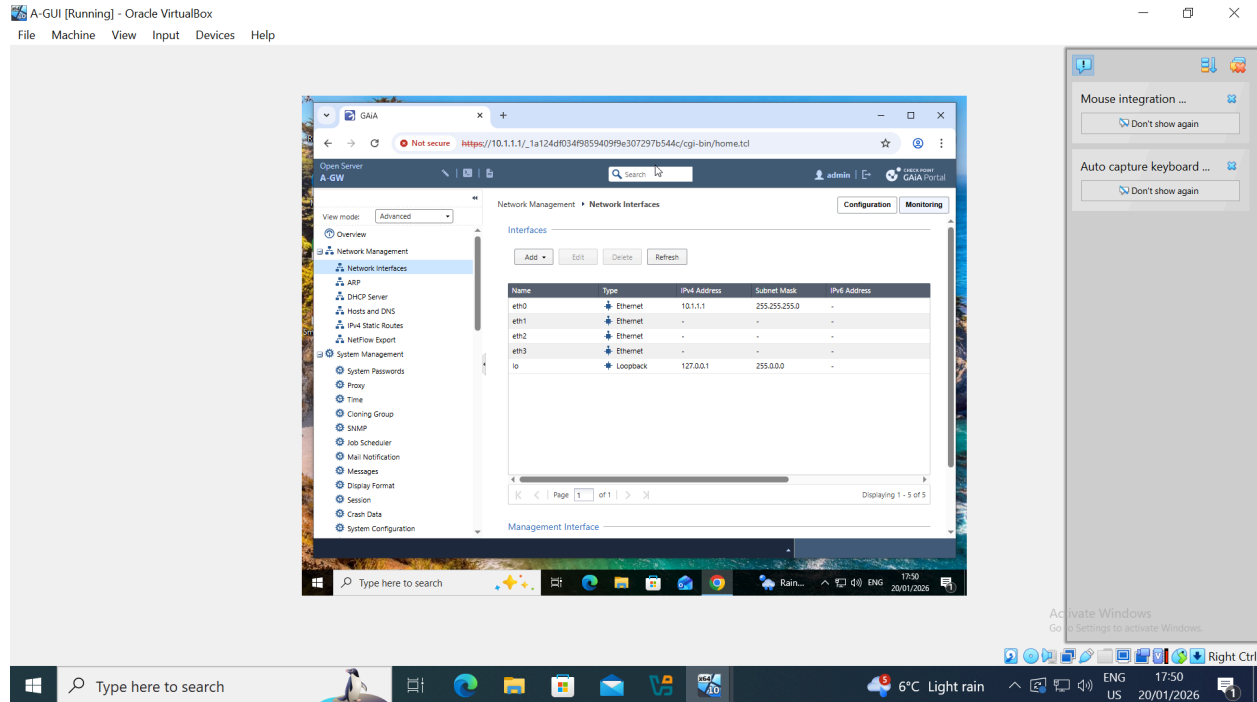
## After Install License



The Security Gateway (A-GW) and Security Management Server (A-SMS) are now fully licensed and functioning normally following the completion of the license installation procedure. The licence has been correctly attached and activated, as evidenced by the licence status showing OK and no active alarms. The system is now completely operational for policy deployment, traffic inspection, and security monitoring throughout the company network with the firewall and monitoring blades active on the gateway.

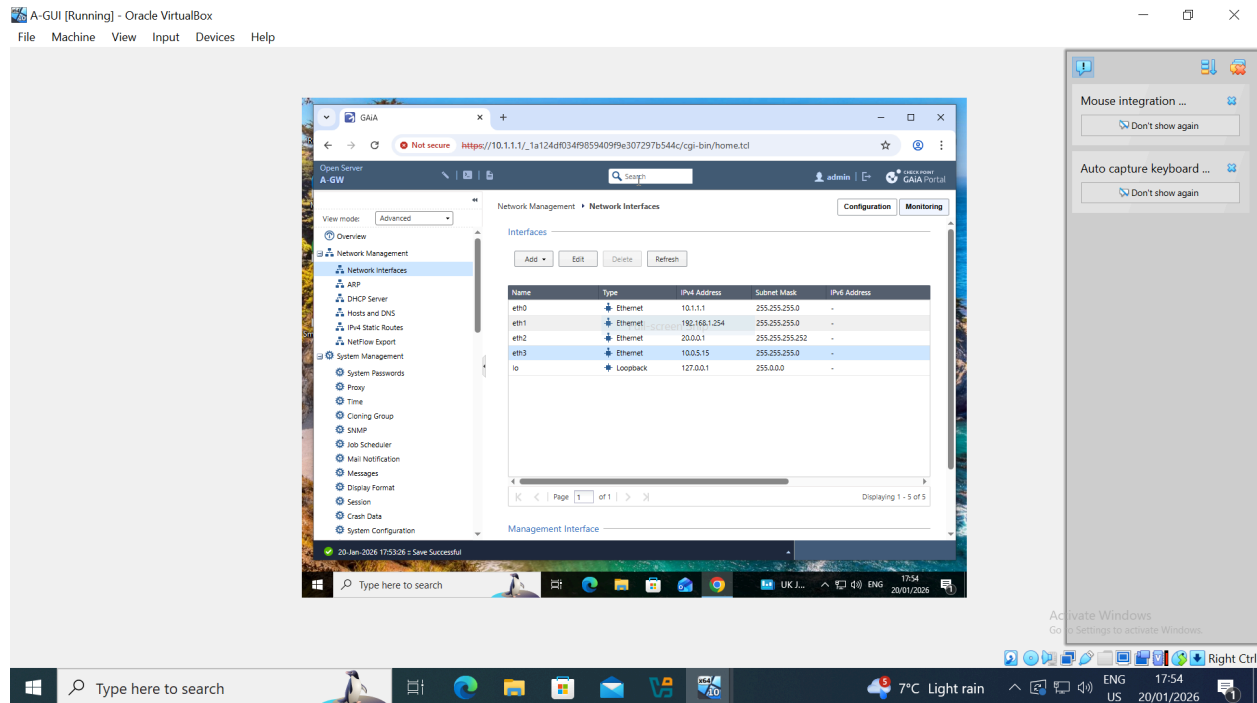
# Network Interface Configuration

## Before:



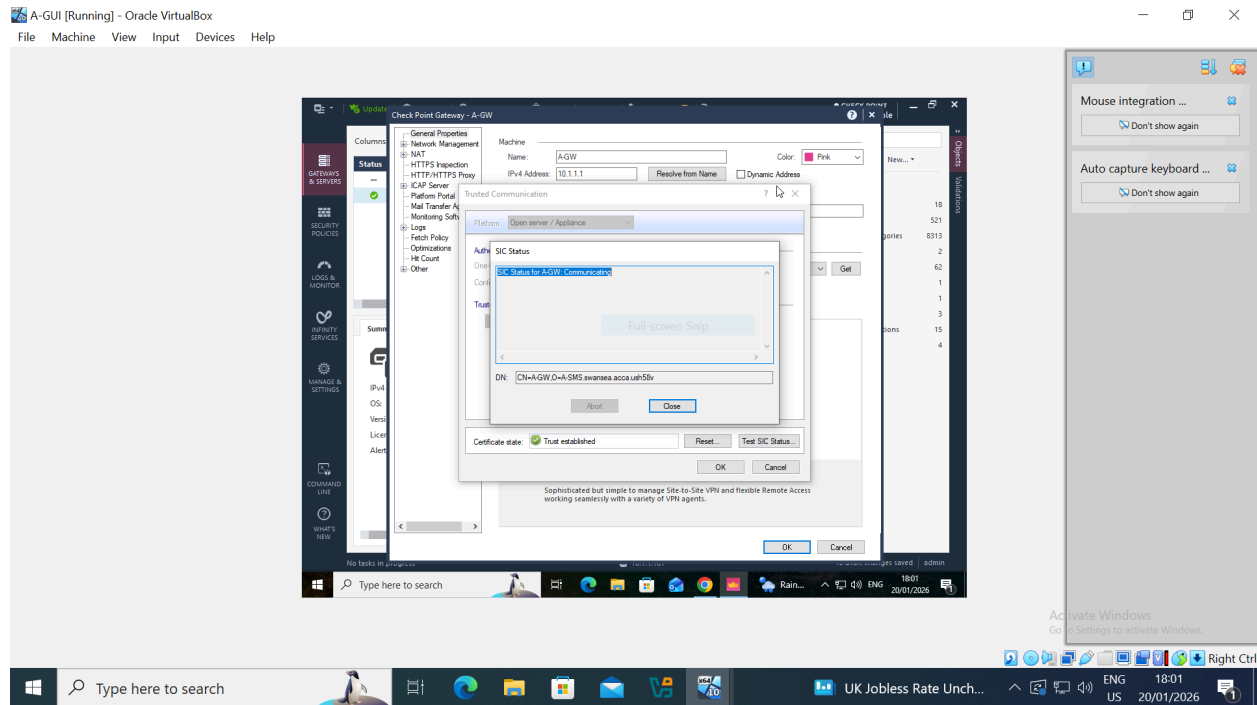
With just the administration interface (eth0) set up, the Security Gateway (A-GW) was initially reachable via the GAiA Web Portal. Although they were accessible, the remaining interfaces (eth1, eth2, and eth3) lacked IP addresses. The gateway was installed and accessible at this point, but it was not yet linked to either the internal or external networks.

## After:



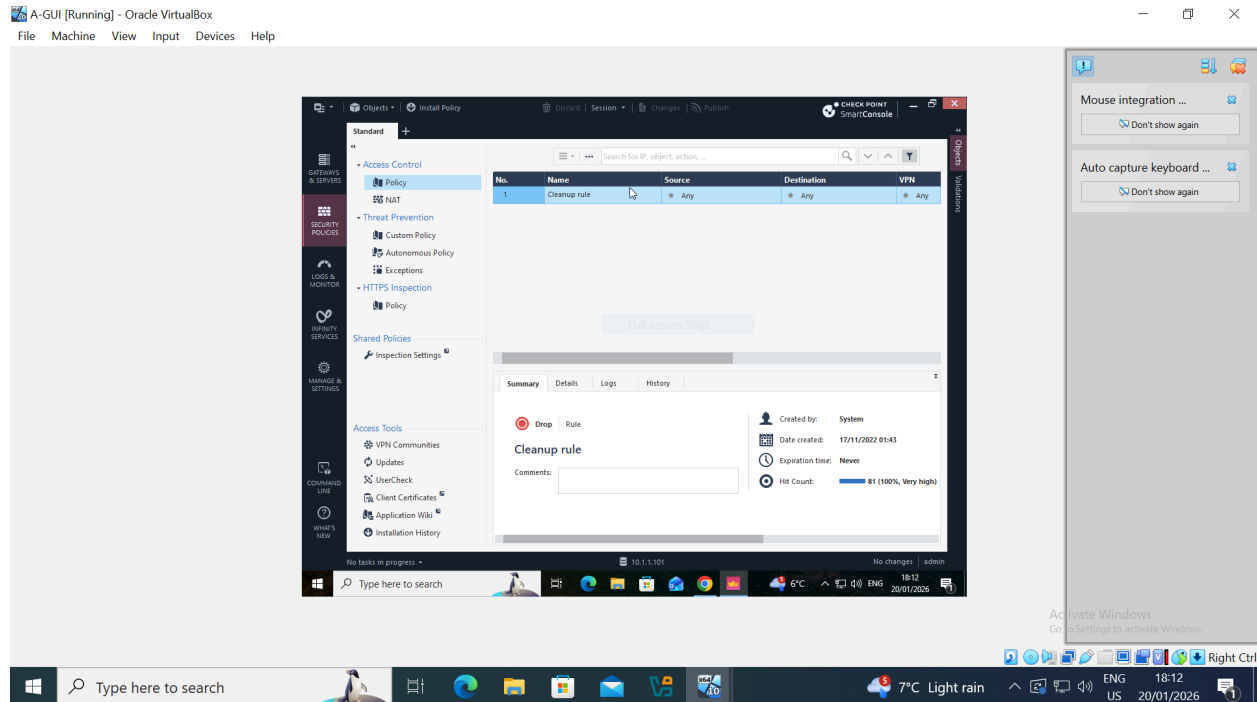
IP addresses were successfully allocated to several interfaces following network interface configuration, allowing for appropriate network segmentation. The inter-DC links, external network, and internal network were all connected to the gateway. The A-GW was able to completely function as an enterprise security gateway, enforce security policies, and examine traffic thanks to this setup.

## Secure Internal Communication (SIC) – Established Successfully



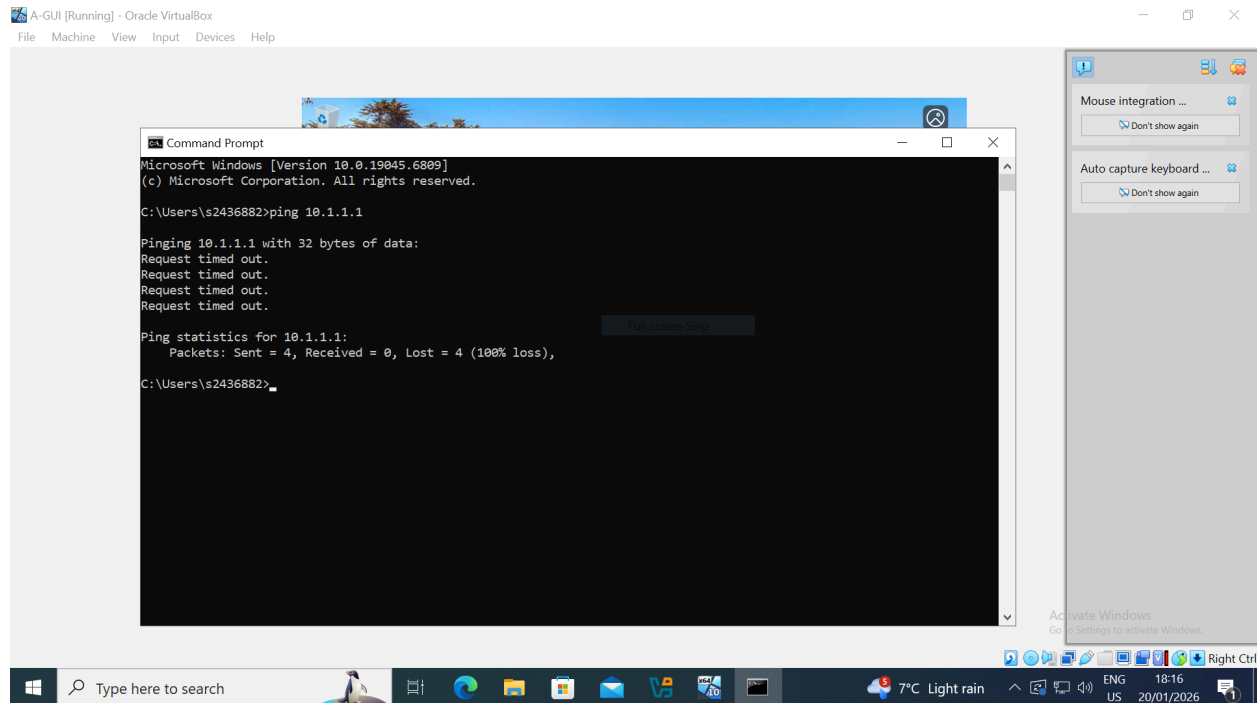
The Security Gateway (A-GW) and the Security Management Server (A-SMS) have successfully established Secure Internal Communication (SIC). A trusted and encrypted channel between the gateway and the management server is active, as shown by the SIC status of "Communicating." This enables the gateway to consistently receive and implement security policies by guaranteeing secure policy installation, monitoring, and administration activities.

## Before Security Rules Configuration



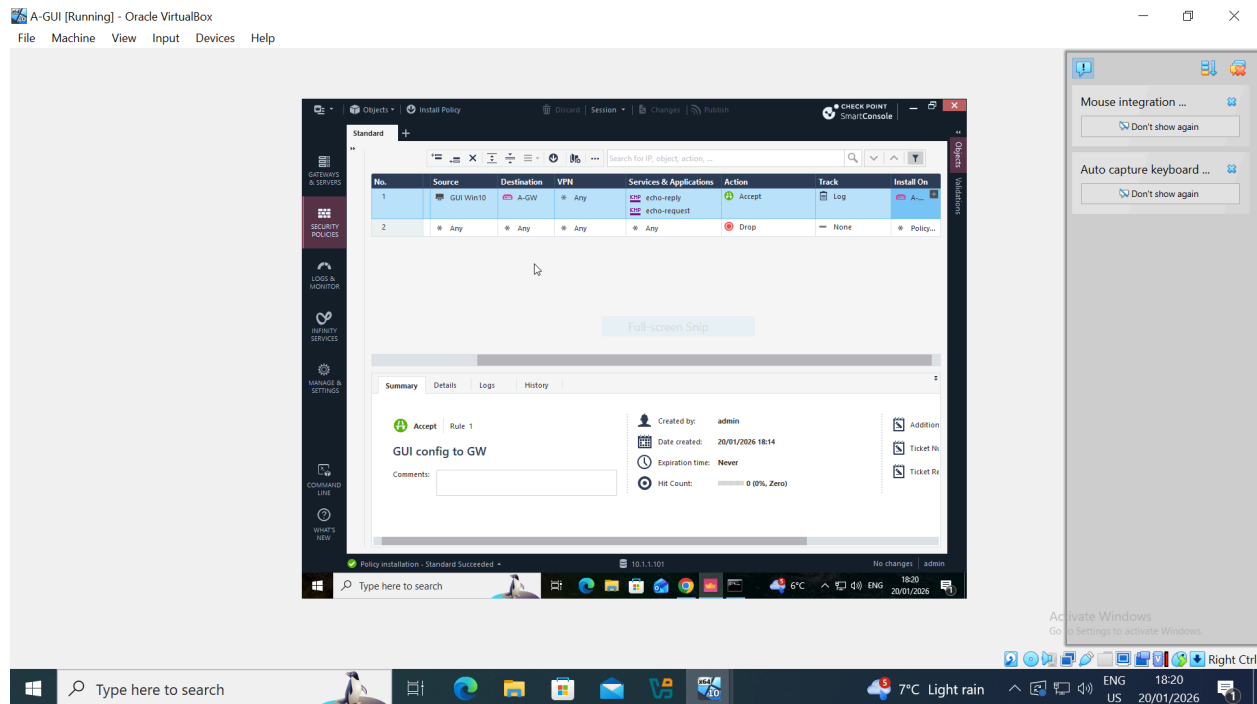
The Access Control policy only included the default Cleanup Rule prior to implementing any custom security rules. All traffic that does not match any expressly defined rule will be dropped by this rule. Since there were no explicit allow or deny rules in place at this point, all network traffic was automatically prohibited. Before specifying specific security policies, this first configuration guarantees a secure baseline posture.

## Connectivity Test (Before Applying Security Rules)



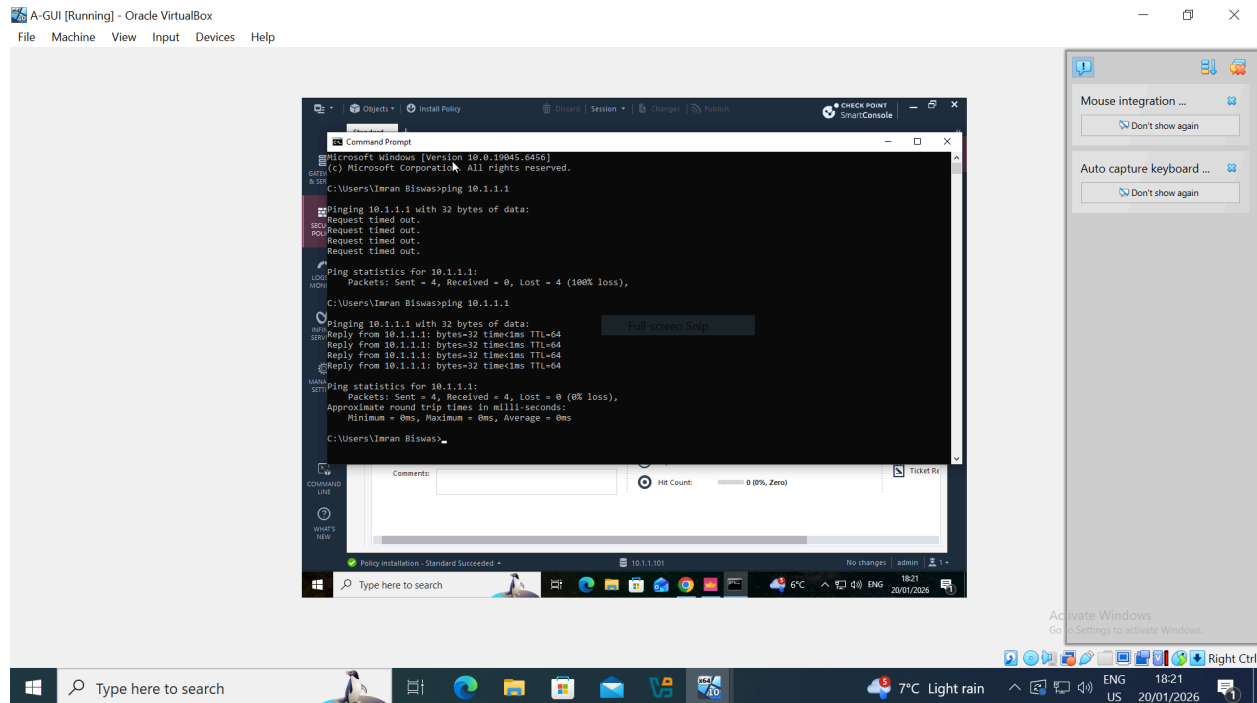
A connectivity test was carried out using the ping command from the GUI computer to the Security Gateway (A-GW) prior to applying any security rules. The traffic was banned, as evidenced by the ping requests' 100% packet loss. Since only the default cleanup rule (drop all) was in effect at this point, this behavior was to be expected. The outcome demonstrates a secure default-deny posture by confirming that no traffic is permitted prior to explicitly setting security rules.

## After Applying GUI to Gateway Rule



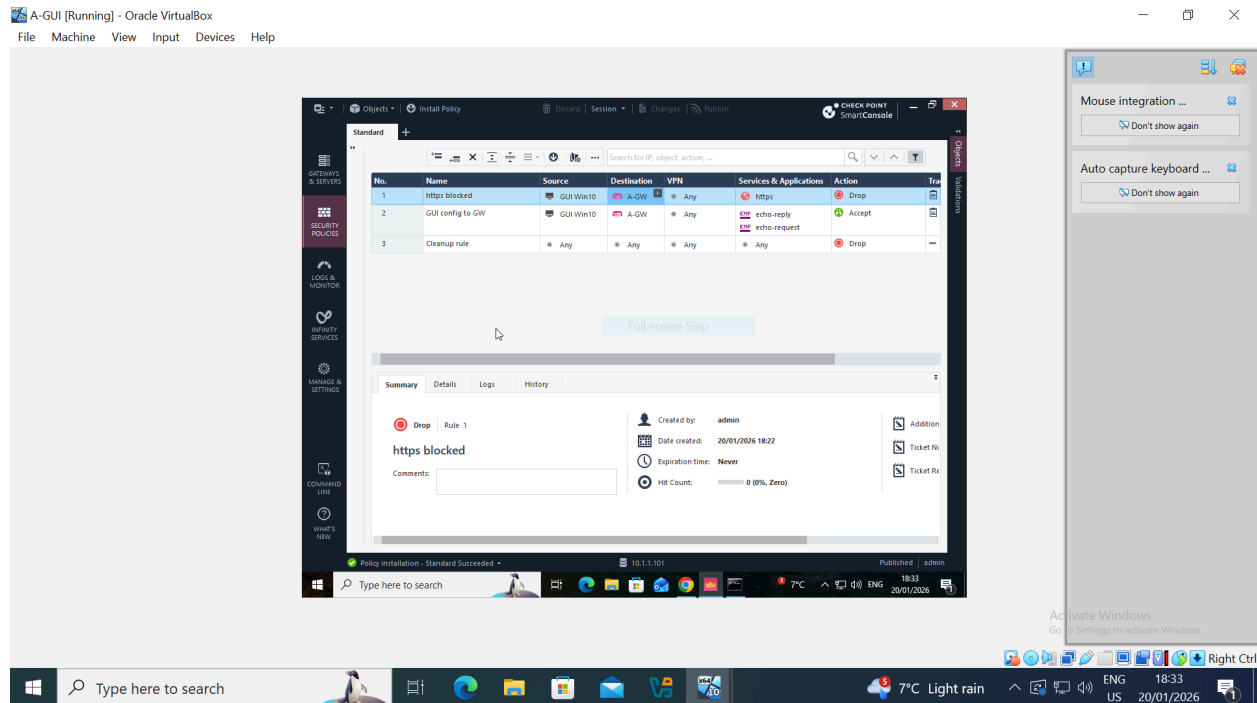
Connectivity was successfully established after a certain security rule was added to permit communication from the GUI machine to the Security Gateway (A-GW). While the housekeeping rule continues to prohibit all other traffic, an access control rule was set up to allow ICMP (echo-request and echo-reply) traffic from the GUI to the gateway. The policy was implemented successfully, indicating that the firewall is enforcing rules as expected and that controlled access is now permitted.

## Successful Connectivity Test



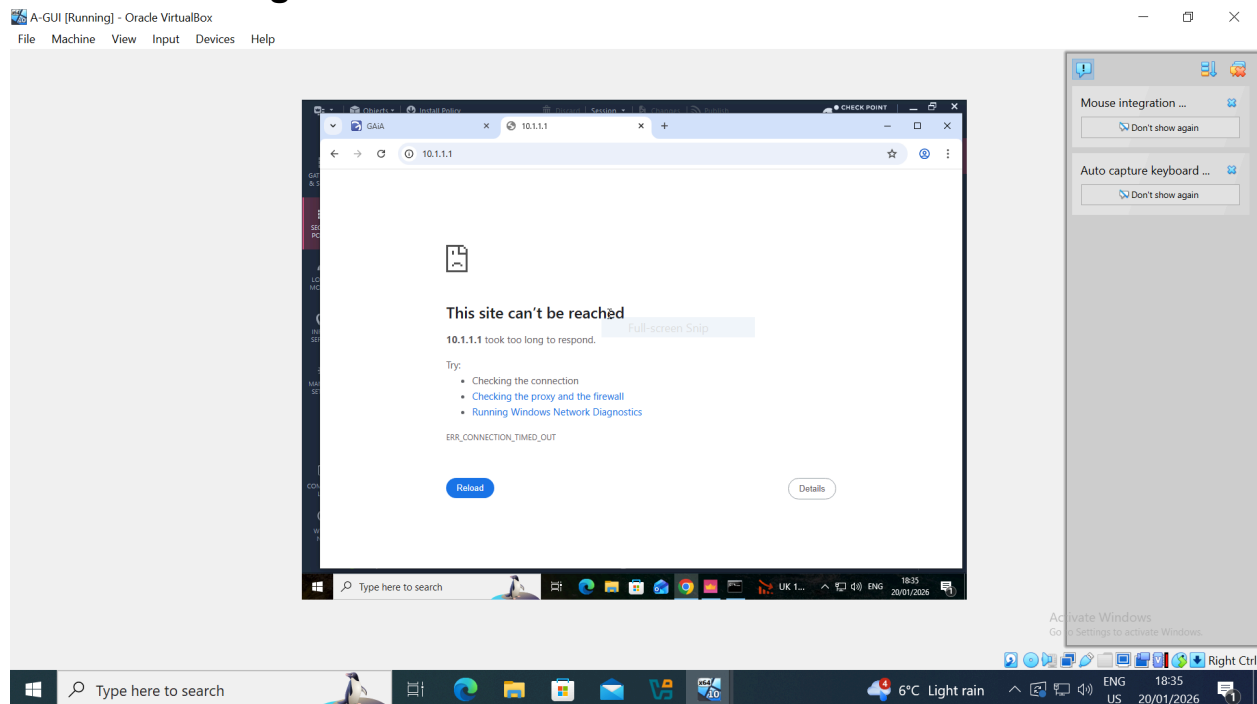
A connectivity test was conducted using the ping command from the GUI computer to the Security Gateway (A-GW) following the installation of the new security policy. All packets were received and there was no packet loss during the successful ping, indicating that the newly set up access control rule is operating as intended. This outcome confirms that while other traffic is still blocked in accordance with the security policy, ICMP traffic is now allowed as planned.

## HTTPS Traffic Control Rule

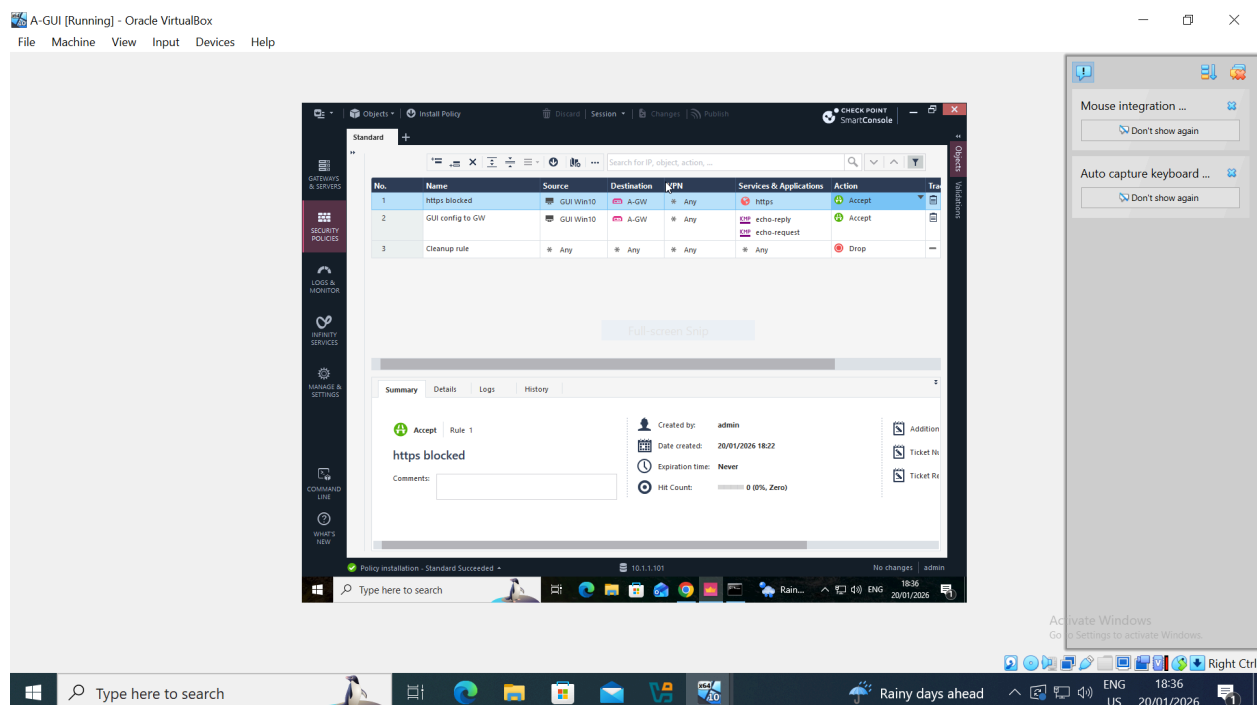


To control HTTPS traffic between the GUI machine and the Security Gateway (A-GW), a particular security rule was added to the Access Control policy. Only necessary ICMP traffic is permitted through a different rule, whereas HTTPS traffic from the GUI to the gateway is expressly blocked by the rule. Fine-grained control over application-level traffic was demonstrated when HTTPS access was successfully restricted as planned after the policy was published and installed. The cleanup rule still applies to all other unidentified traffic.

## Blocked Testing Result



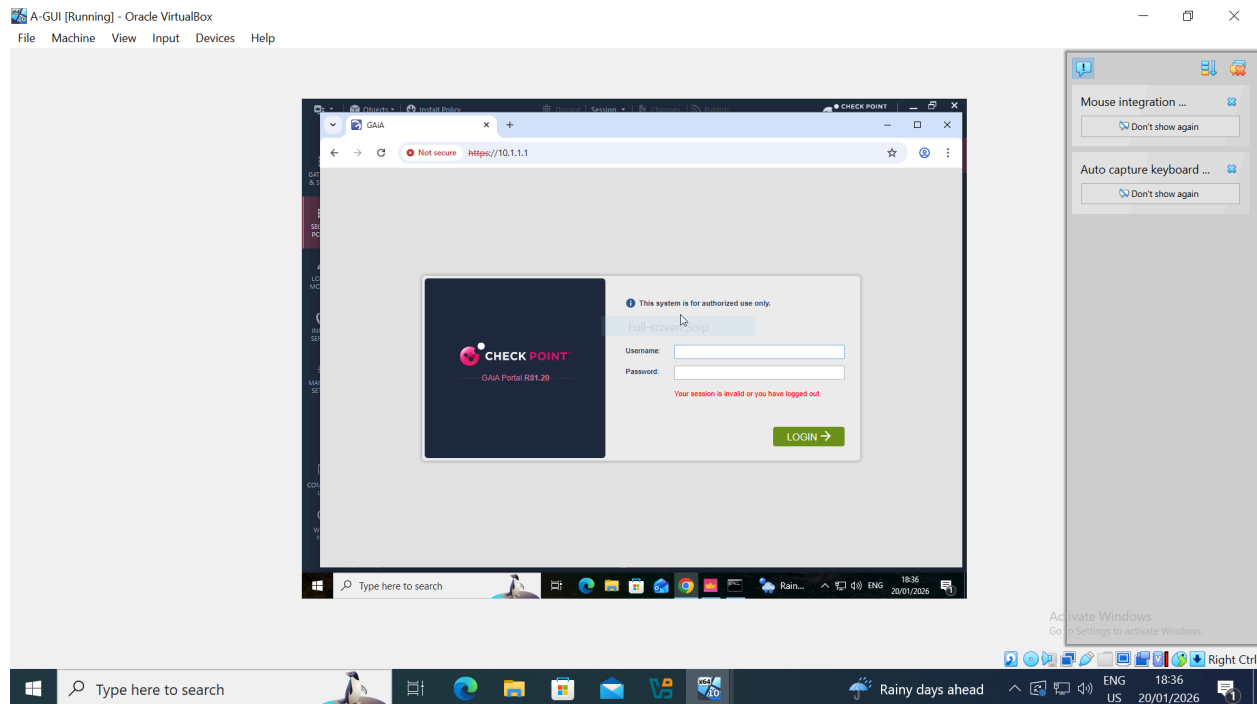
## HTTPS Access Rule



To permit HTTPS traffic from the GUI computer to the Security Gateway (A-GW), a specific access control rule was set up. HTTPS access was successfully allowed when the policy was published and installed, but the

cleanup rule still banned other unspecified traffic. This exhibits exact rule-based control, guaranteeing authorized and safe HTTPS communication with the gateway while upholding a robust default-deny security posture.

## Web (HTTPS) Access – Successfully Enabled



Web access to the Security Gateway (A-GW) was successfully created after setting up and implementing the HTTPS allow rule. The GAiA Web Portal may now be accessed using HTTPS, demonstrating that the access control policy is appropriately allowing authorized web traffic while upholding security limitations for other services. This illustrates regulated administrator access to the gateway and efficient policy enforcement.

## **Conclusion**

Check Point GAIa appliances were used in this lab to successfully design, deploy, and validate an enterprise network security infrastructure. The Security Management Server (A-SMS) and Security Gateway (A-GW) were successfully added and integrated, and the SmartConsole was installed correctly. In order to ensure secure and encrypted communication between management and gateway components, Secure Internal Communication (SIC) was established.

The gateway's network interfaces were set up to facilitate appropriate network segmentation, allowing for both internal and external access. The default-deny approach was then used to build security controls. In order to ensure a secure baseline, early connectivity tests verified that traffic was stopped prior to imposing rules. Controlled ICMP and HTTPS communication from the GUI to the gateway was successfully permitted after particular access control rules were defined; all other traffic was kept limited by the cleanup rule.

Effective rule enforcement was shown during policy installation and testing, with successful ping and web access verifying proper configuration. Overall, this lab reflected actual company network security procedures by offering hands-on, practical experience with enterprise firewall configuration, secure communication setup, and policy-based traffic control.