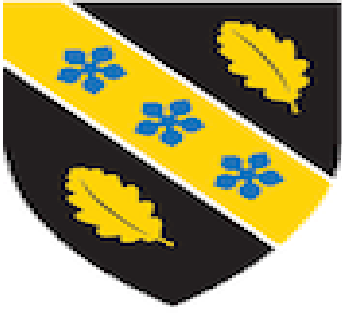




Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

***Name:** Harsh Rameshkumar Mangukiya*

***Student ID:** 2433852*

***Assignment title:** Securing the Enterprise Network Implementation of a Network Security Solution*

Table of Contents

1. INTRODUCTION AND NETWORK SECURITY CONTEXT	4
1.1 Overview	4
1.2 Security Implementation Scope	4
1.3 Report Structure	4
2. CHECK POINT SECURITY INFRASTRUCTURE DEPLOYMENT	5
2.1 Network Topology Modification and Design Rationale	5
2.2 Gaia Operating System Installation	5
2.2.1 A-SMS Installation and Base Configuration.....	5
2.2.2 A-GW Installation and Network Interface Configuration.....	6
2.3 First Time Wizard Configuration	8
2.3.1 Security Management Server (A-SMS) Configuration.....	8
2.3.2 Security Gateway (A-GW) Implementation	9
2.4 SmartConsole Installation and Configuration.....	11
2.5 Security Gateway Object Creation and SIC Establishment.....	13
2.5.1 Gateway Object Creation Using Wizard Mode	13
2.5.2 Secure Internal Communication (SIC) Verification.....	14
2.6 License Management and Activation.....	14
2.6.1 License Requirements Analysis	14
2.6.2 License Installation via SmartUpdate	14
2.6.3 Service Contract Updates.....	15
2.6.4 License Status Verification and Documentation	15
3. FIREWALL POLICY IMPLEMENTATION AND TRAFFIC CONTROL	16
3.1 Enterprise Security Policy Framework	16
3.2 Firewall Rule Base Design and Architecture	16
3.3 Inbound Traffic Rules Configuration.....	17
3.3.1 ICMP Traffic Control.....	17
3.3.2 HTTP/HTTPS Web Traffic Rules	17
3.3.3 SSH Remote Administration Control.....	18

3.3.4 FTP Service Restrictions.....	18
3.3.5 Telnet Protocol Blocking	18
3.4 Outbound Traffic Rules Configuration	18
3.4.1 Internet Access for Internal Users.....	18
3.4.2 Email and Communication Services.....	18
3.4.3 Outbound Administrative Traffic	19
3.5 Inter-Site VPN Traffic Rules.....	19
4. ENHANCED SECURITY FEATURES IMPLEMENTATION	19
4.1 Proposed Additional Security Enhancements	19
4.2 Intrusion Prevention System (IPS) Configuration	20
4.2.1 IPS Profile Creation and Assignment	20
4.2.2 IPS Rule Integration.....	20
4.3 Application Control and URL Filtering	20
4.4 Identity Awareness and User-Based Access Control	21
4.5 Anti-Malware and Anti-Bot Protection.....	21
5. TESTING, VALIDATION, AND OPERATIONAL VERIFICATION.....	21
5.1 Connectivity Testing	21
5.2 Firewall Rule Testing Methodology	22
5.3 Enhanced Security Feature Validation	22
6. CONCLUSION AND SECURITY POSTURE ASSESSMENT.....	22
6.1 Implementation Summary.....	22
6.2 Operational Considerations and Future Enhancements	23
7. REFERENCES	24

1. INTRODUCTION AND NETWORK SECURITY CONTEXT

1.1 Overview

This report reports the Part 2, which is safeguarding the enterprise net by applying a network security solution using Check Point Gaia appliances. The current environment comprises of two locations which are SWANSEA.ACCA and LONDON.SWANSEA.ACCA with its core services, which include DNS, Active Directory, VPN, DHCP, IIS, firewalls as part of Part 1. Introduction of Check Point Security Management Server using SmartConsole, will result in a central point of conducting security policy management, monitoring, and updates, as well as imposing justified controls on inbound and outbound traffic. The work addresses the Learning Outcome 1 because it employs the concept of unified security management to control and monitor traffic and Learning Outcome 2 because it empowers the security service and implements security policies to address some of the major technical vulnerabilities.

1.2 Security Implementation Scope

The report addresses three areas of implementation that are needed in part 2 of the evaluation. First, it incorporates Check Point Security Management Server and SmartConsole on a GUI and a Security Gateway into the current enterprise network to centralise the policy management and monitoring as well as updates. Second, it establishes and implements both inbound and outbound firewall controls, which is justified through an enterprise security policy framework that is reflective of the actual organisational needs in real sense. Third, it suggests and makes realised other security services on the basis of Gaia appliances which are in accordance with the recognised industry standards and official guidelines of Check Point. In the event where appropriate, the policy rationale may state commonly accepted frameworks like NIST and ISO/IEC 27001 [1], [2], [3], [4].

1.3 Report Structure

This report is structured in such a way that all the requirements can be found within a short duration of time. Section 2 shows the installation and integration of the Check point Security management server, Security gateway and Smart console management workstation. The firewall policy is discussed in section 3, which seeks to emphasise on justifiable inbound and outbound traffic policies. Section 4 explains other security measures that were put in place to enhance the enterprise network. The evidence is recorded in the form of screenshots of the configurations where timestamps are evidently displayed, and embedded into the report. Every configuration option is supported through its association with security targets, operation requirement and risk minimization.

2. CHECK POINT SECURITY INFRASTRUCTURE DEPLOYMENT

2.1 Network Topology Modification and Design Rationale

The network topology is extended with the addition of Check Point Security Management Server, Security Gateway and SmartConsole management work station to allow centralised security policy, monitoring and updates in the enterprise network. Its design will consist of the following A-SMS with 10.1.1.101/24/eth0, A-GW with 10.1.1.1/24, 192.168.1.254/24, 20.0.0.1/30, and 20.0.0.30, eth2, eth3, and A-UI with 10.1.1.20/24 to access the IP administration. The architecture on which this is based is in line with the Part 2 requirement to administer security policy on the SMS through SmartConsole and not by administering the enforcement alone on the gateway. It can be integrated with the existing domain services, which contain an Active Directory, a child domain and user accounts that can be utilized in role-based access controls implements roles and privileges at the explicit request of users where the service is applied.

A-SMS finds its place within the network management segment to ensure that security management and administration as well as policy management operations are logically removed out of the user production processes. A-GW is placed in a manner that it puts internal and external networks to ensure inbound and outbound controls through which it serves as the main inspection and policy enforcement location. Isolating management traffic and production traffic allows minimizing of irrelevant exposure of administrative services and maintains a distinct separation between operations of policy control and monitoring.

2.2 Gaia Operating System Installation

2.2.1 A-SMS Installation and Base Configuration

A-SMS virtual machine is configured with proper specifications to make it fulfill the functionality of security management such as checking whether the version is configured to be otherUnknown64-bit before turning it on. Gaia R81.20 is installed by simply mounting the image of the GaiaOS.iso [5], [6] and when the boot screen is presented, the user should choose the option of installing Gaia on this system. Screenshots are used to show the installation wizard process did in installing into Great Britain as the keyboard language choice, and the partitions set up window which partitions disk space based on the install system settings without the ability to modify the partition settings. The account of administrator is generated at the time of installation and there is a different maintenance administrator password which is assigned to recover the system. The eth0 network interface is set to a default gateway of 10.1.1.1, IP address 10.1.1.101, netmask 255.255.255.0, default gateway 10.1.1.1 and DHCP is off. After installation and re-booting, the session-timeout values are configured to 720 minutes of both inactivity and web session-timeout time by using set inactivity-timeout 720 set web session-timeout 720 and the values are saved with the command save config.

2.2.2 A-GW Installation and Network Interface Configuration

A-GW is also installed in the same way as Gaia R81.20, with eth0 set to 10.1.1.1/24 setting at install. With the completion of First Time Wizard, three further interfaces are set up to separate the traffic by purpose with eth0, the management interface, comment Swansea.acca, eth1 192.168.1.254 /24 comment IntSWA serving internal Swansea traffic, eth2, 20.0.0.1 /30 comment ExtLCD able to be accessed as an external iPconnectivity link, and eth3 comment ExtInt, which is provided with an IPv4 address automatically via DHCP. Separated routing and protection of management, internal user traffic, internal site to internal site connections and external internet access is possible and the interface segregation allows separate risk control measures in places where two or more trust areas face cross-contamination threats.

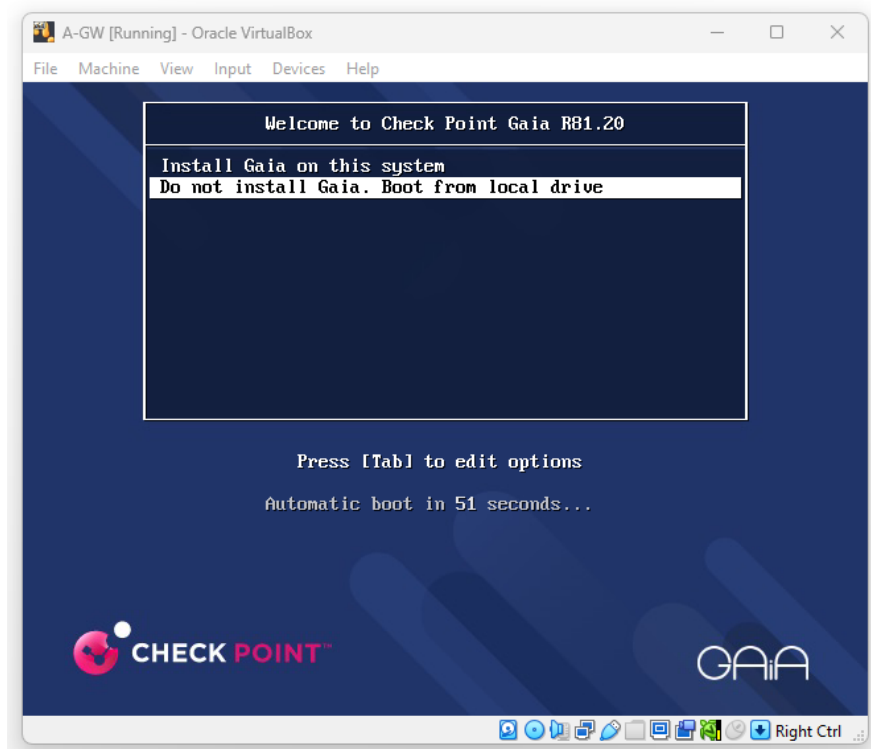


Figure 1: Gaia R81.20 Boot Screen Installation Options

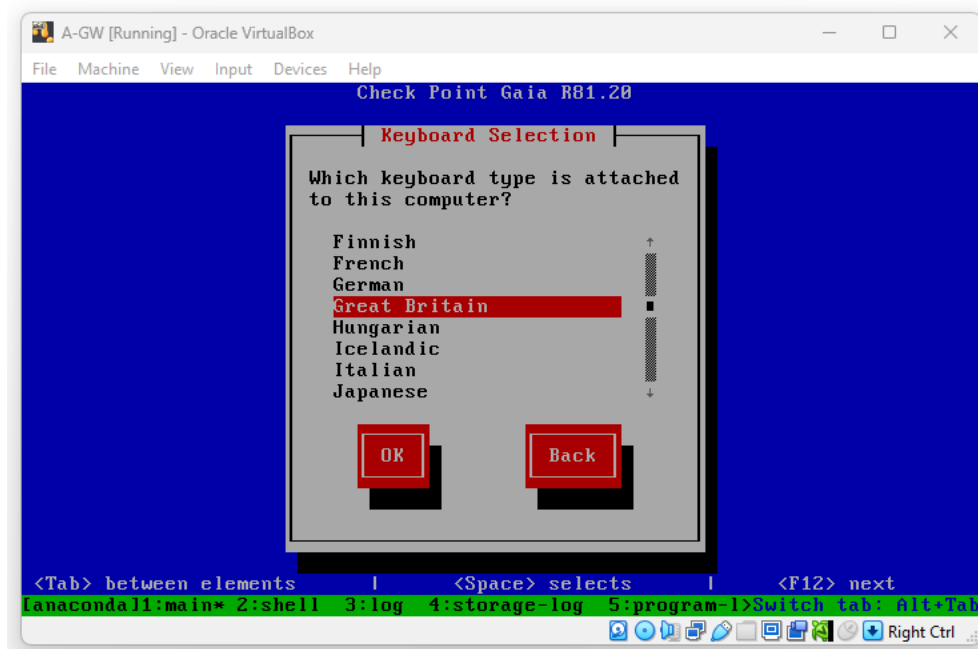


Figure 2: Keyboard Selection Great Britain Configuration

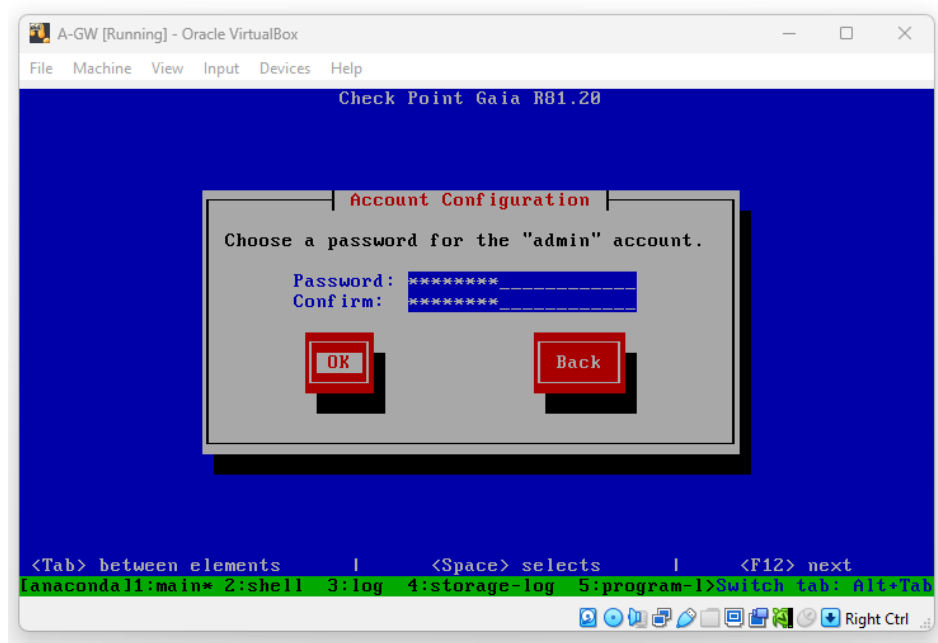


Figure 3: Admin Account Password Configuration Screen

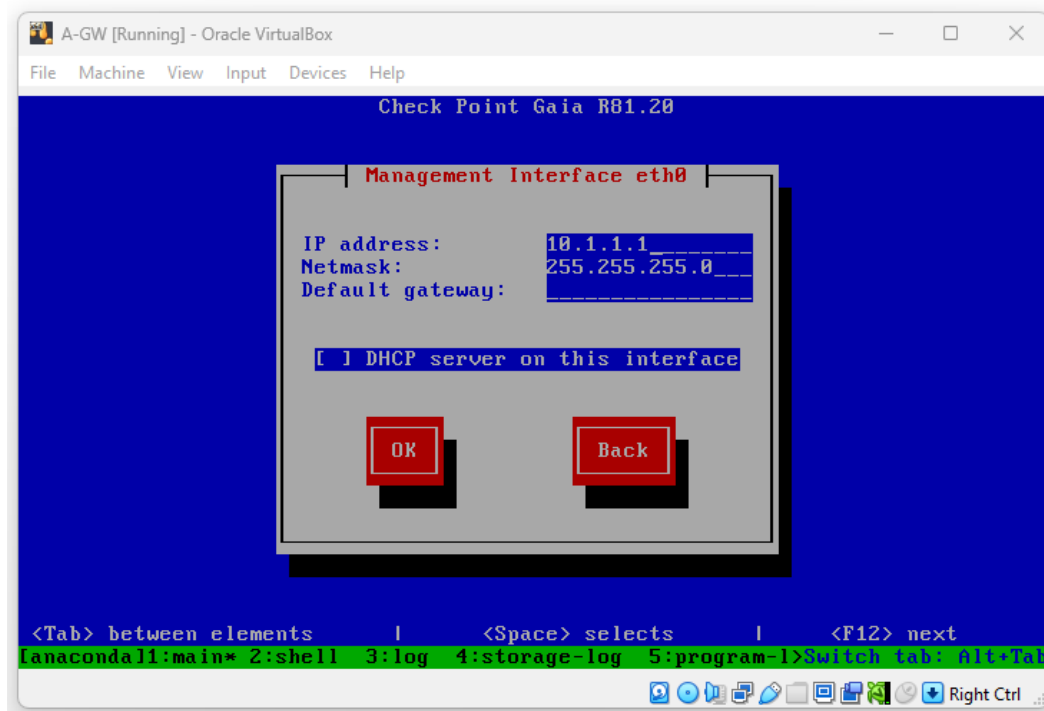


Figure 4: Management Interface eth0 IP Configuration

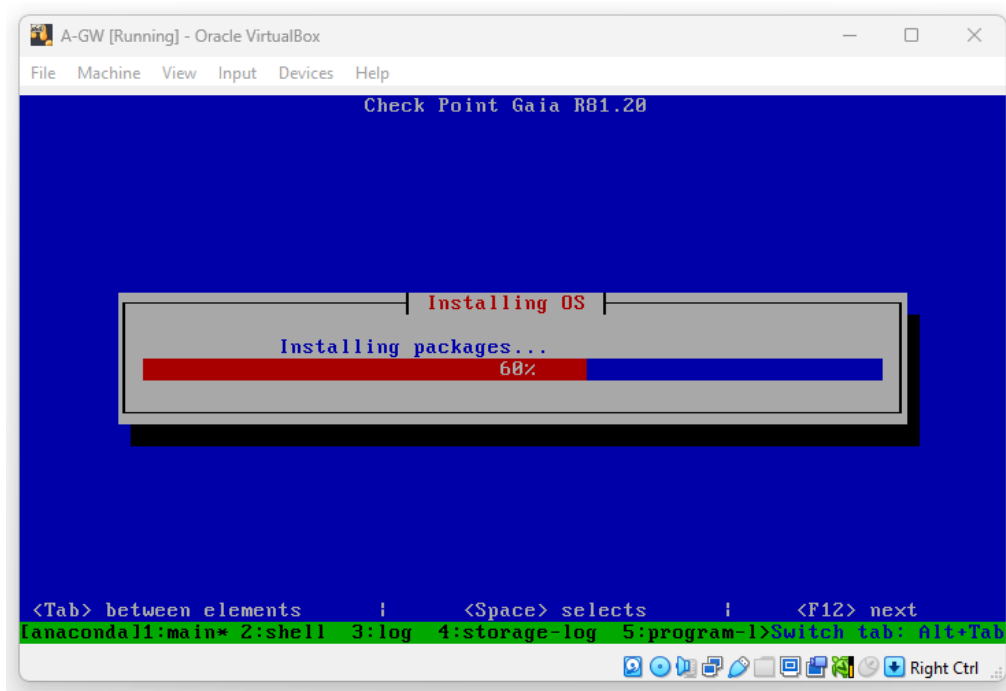


Figure 5: Gaia OS Installation Progress at 68%

2.3 First Time Wizard Configuration

2.3.1 Security Management Server (A-SMS) Configuration

First Time Wizard will be opened in A-GUI through a browser (open <http://10.1.1.101>) where the administration credentials created in the course of installation will be used. Upon choosing the next step as R81.20 configuration, one will be asked to confirm the settings related to management connection settings. The settings of the device information are set to hostname A-SMS, domain name swansea.acca, and primary

DNS server 192.168.1.1 (domain controller), secondary DNS 8.8.8.8, and tertiary DNS server 4.2.2.2. The Date and Time Settings page has Network Time Protocol which is turned on and time1.google.com as the primary and time2.google.com as the secondary NTP server and finally time zone London, Europe GMT. The option will be Security Gateway and / or Security Management whereby the Security Management option will be selected and the configuration will be Primary Security Management. New administrator account is made with user name cpadmin and a password of choice to log in SmartConsole. The network option is chosen on the Security Management GUI Clients page using IP address 10.1.1.0 and subnet 255.255.255.0 which limits access to SmartConsole to the management network part only which lowers the risk of exposure to unauthorised administrative access. Once it has finished the wizard, the terminal is entered on which the command api status will be executed until the API readiness test is successful, which will show that A-SMS startup processes are finished and the SmartConsole connection is made.

2.3.2 Security Gateway (A-GW) Implementation

A-GW uses the First Time Wizard that is reached through the use of the 10.1.1.1 address through A-GUI. The settings of device information are configured with A-GW as a hostname, domain swansea.acca and the same DNS servers as A-SMS. The configuration of NTP synchronization is the same. The Products page attests to Security Management not being turned on and Security Gateway turned on. The gateway is confirmed not to be using dynamically allocated IP. In order to have a secure internal communication, one is required to input the activation key Chkp!234 on the Secure Communication to Management Server page. SIC is a system that makes use of one-time password to be authentic and creates a secure and encrypted channel between the management server and the gateway which is necessary in the distribution of the policies and monitoring them safely.

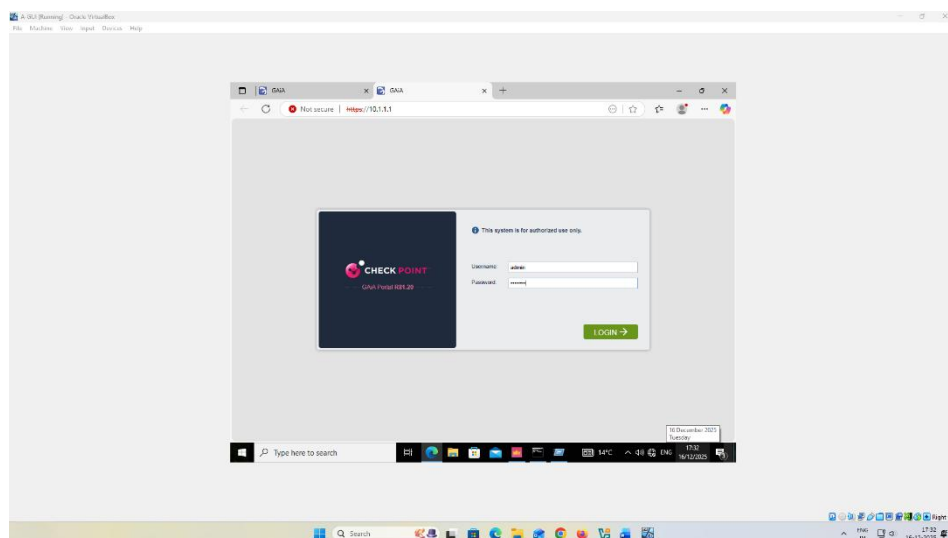


Figure 6: Gaia Portal Login Screen After Restart

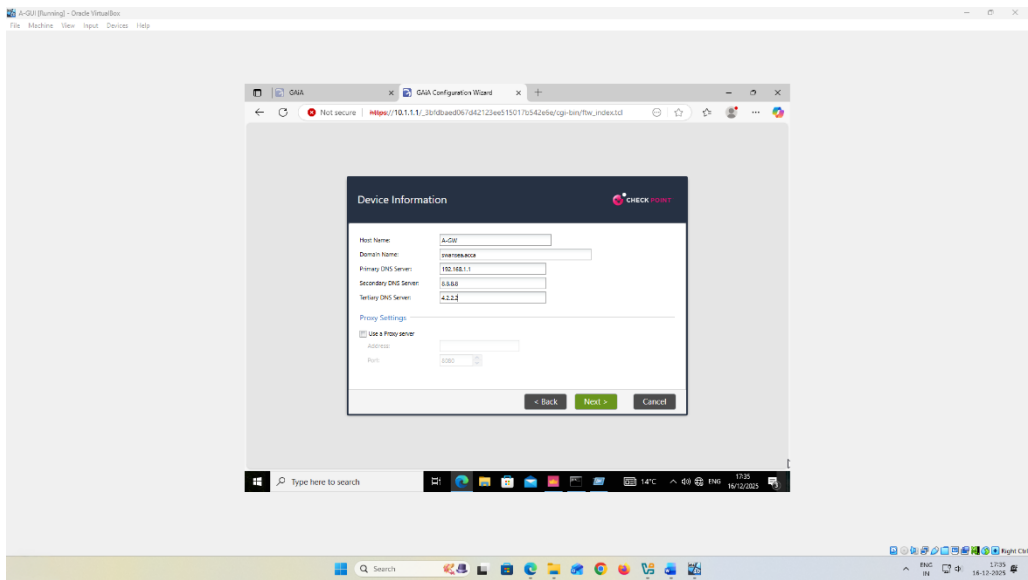


Figure 7: Device Information Configuration for A-GW

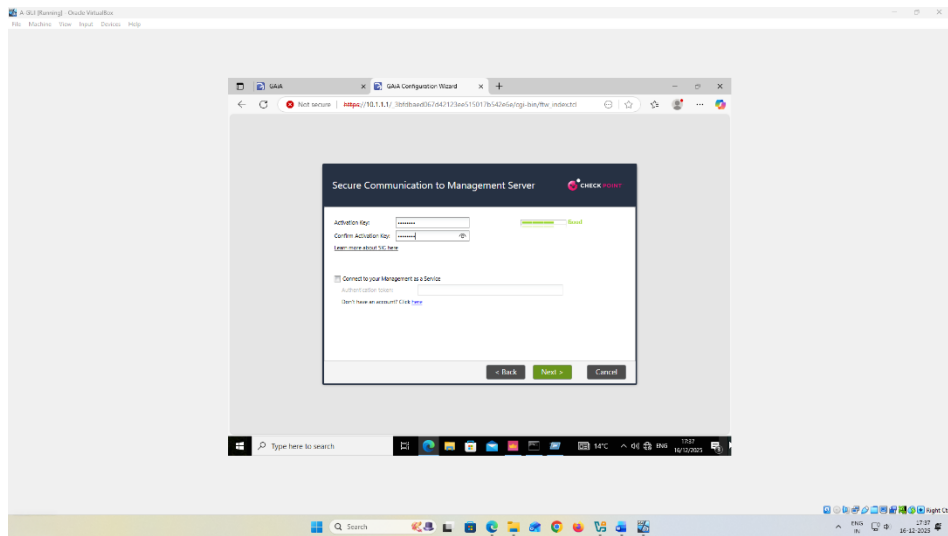


Figure 8: SIC Activation Key Entry Screen

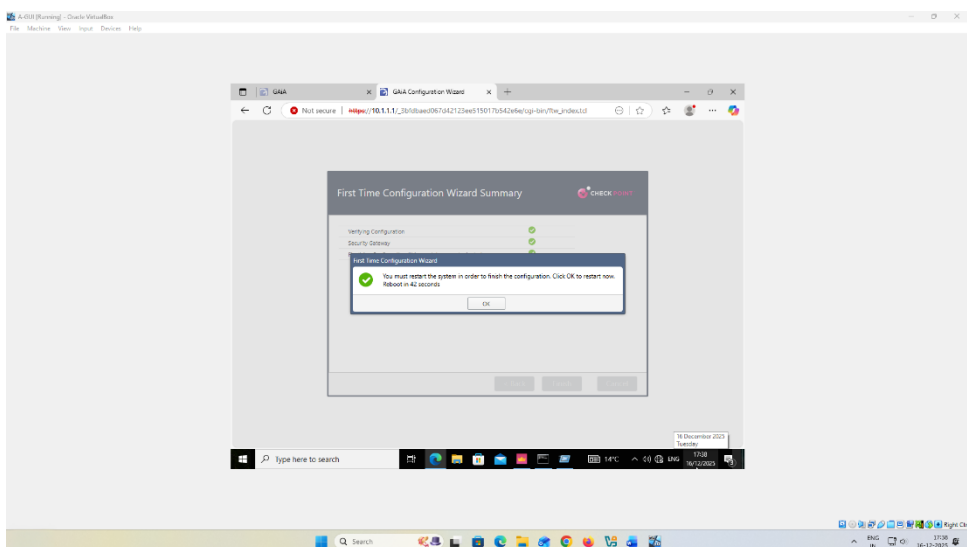


Figure 9: First Time Wizard Configuration Summary

2.4 SmartConsole Installation and Configuration

The A-GUI workstation gets SmartConsole R81.20 installed, by calling CheckPointR81.20_SmartConsole.exe installer that is already in the Downloads folder. Once the Check Point End User License Agreement is possible to agree with, installation is done, and when this is completed, Smart Console R81.20 is available in the A-gui desktop.

The first one will be set up by opening SmartConsole and typing the IP of the server 10.1.1.101, username cpadmin and the password that had been generated during the First Time Wizard administrator account creation. There is a fingerprint verification dialog on initial connection to server 10.1.1.101 that on comparison of the displayed fingerprint with recognizable accelerator on the server, an administrator is expected to confirm server identity, thus preventing man-in middle attacks. Once the verified fingerprint has been taken, SmartConsole gives a centralized control of the security infrastructure, such as managing policies via the Security Policies view, creating objects, configuration of gateways, monitoring of events, and publishing and installing policies to the managed gateways.

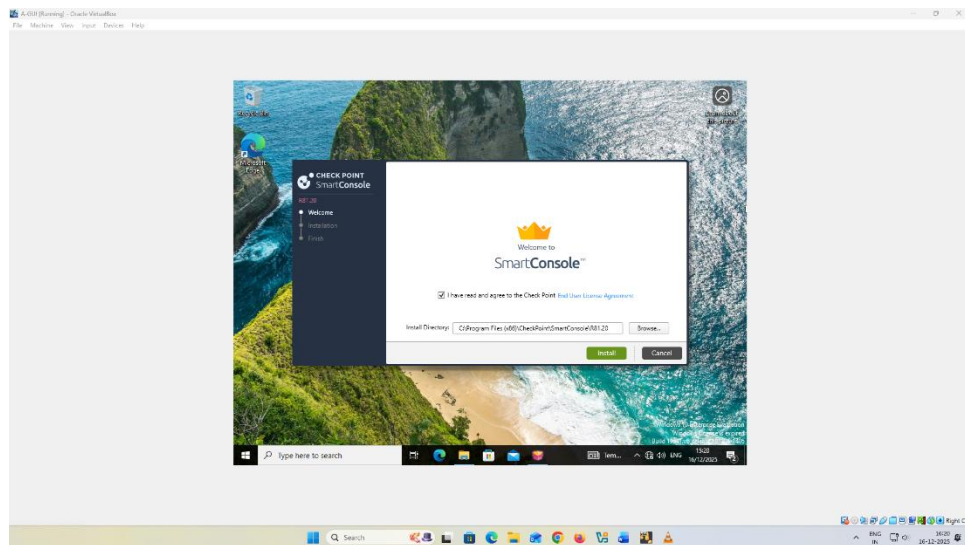


Figure 10: SmartConsole R81.20 Installation Welcome Screen

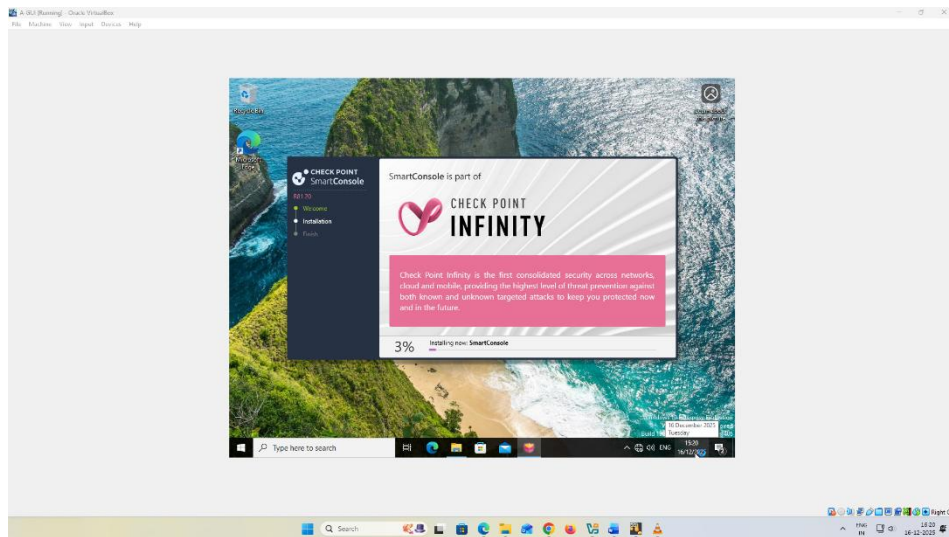


Figure 11: SmartConsole Installation Progress at 3%

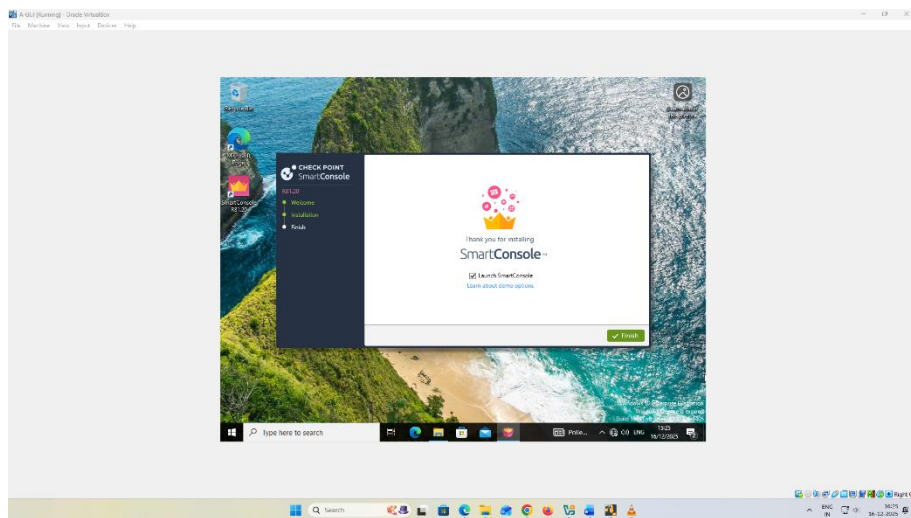


Figure 12: SmartConsole Installation Successfully Completed

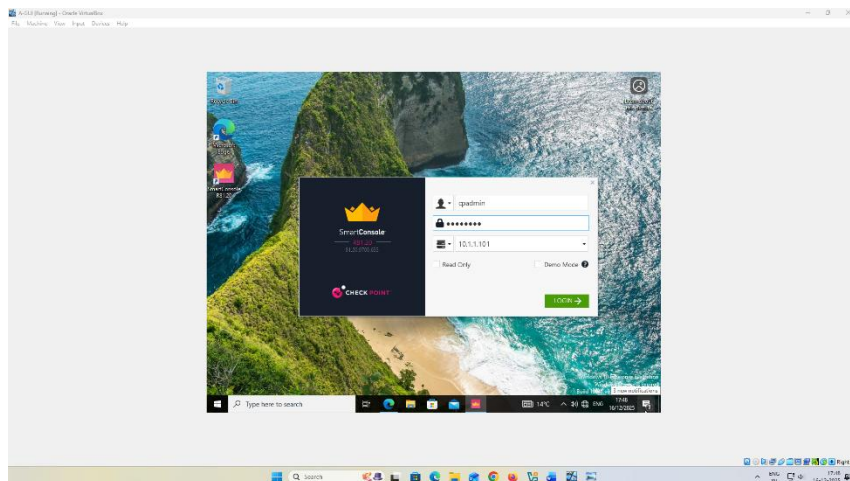


Figure 13: SmartConsole R81.20 Login Screen cpadmin

2.5 Security Gateway Object Creation and SIC Establishment

2.5.1 Gateway Object Creation Using Wizard Mode

Once the SmartConsole provided by A-GUI is entered, a new Gateway object is created by selecting the option of Gateway in the New menu and then option of Wizard Mode is chosen to open the Check Point Security Gateway Creation Wizard. The gateway is set with name A-GW, gateway platform Open server and IPv4 gateway 10.1.1.1. Chkp!234 is the one-time password typed in during secure communication establishment. The Get Topology Results window contains the configuration data, which has been retrieved, configuration of all interfaces, IP addresses of all interfaces and network topologies, which have been verified then the option of Close and followed by Finish is chosen to complete the wizard.

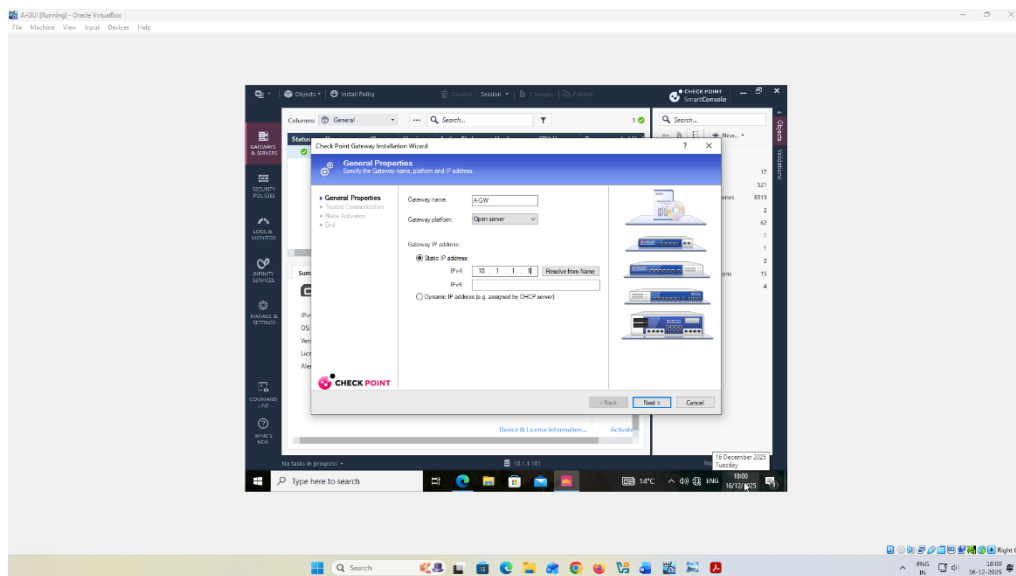


Figure 14: Gateway Creation Wizard General Properties Page

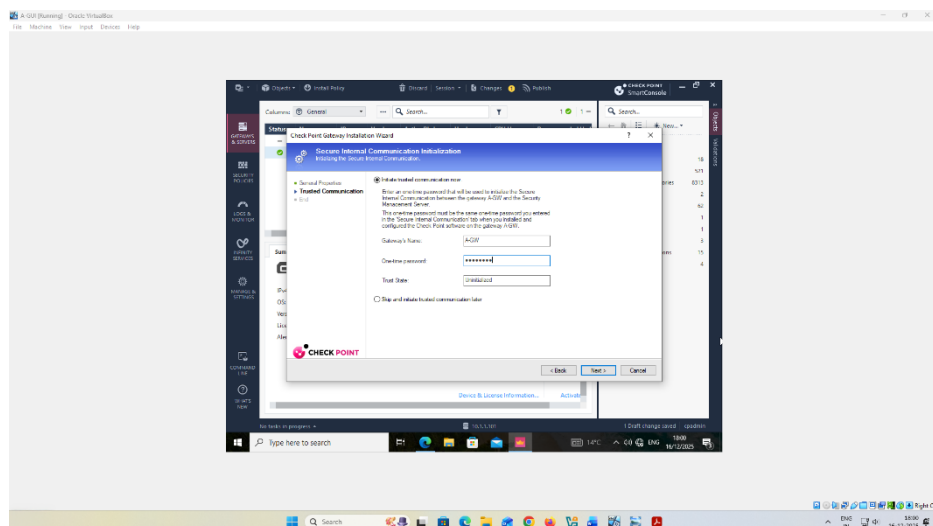


Figure 15: SIC Initialization with One-Time Password

2.5.2 Secure Internal Communication (SIC) Verification

The access to the A-GW object is found at the view of the Gateway Servers and A-GW communication settings is opened at the gateway properties. Test SIC Status button is clicked in order to check the establishment of communication. An effective and well set up SIC shows a status of communicating which affirms that the encrypted trust between SMS and Gateway is running effective to distribute policies and monitor events in a secure manner. This trust relationship will make it impossible to push policies by unauthorized management servers and will also make it impossible to tamper with the communication channels.

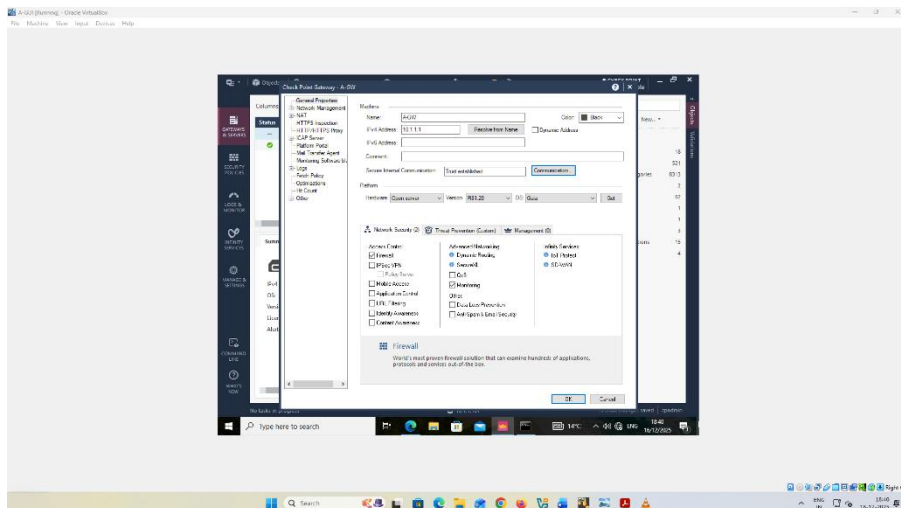


Figure 16: Gateway Properties Showing Trust Established Status

2.6 License Management and Activation

2.6.1 License Requirements Analysis

Analysis of the Requirements of the license. The evaluation will involve the application of the necessary licenses on both the SMS appliances and Check Point appliances based on the guidelines required by the Check Point manuals with the licensing status and the expiry reports documented. The licenses should be such that they allow the necessary security blades to enforce the firewall, intrusion prevention, anti-malware protection and application control making it possible to put security features required in Part 2 into effect.

2.6.2 License Installation via SmartUpdate

SmartConsole accessed SmartUpdate utility from within which licenses are centrally managed. In the case with A-SMS, the license file (A-SMS.lic) is registered into the license repository, and the local license is attached to the object of the Security Management Server, and it funds successful installation. A-GW license (A -GW.lic) is also put in the repository and is assigned to the object of the gateway A -GW, which allows the security gateway appliance to enforce.

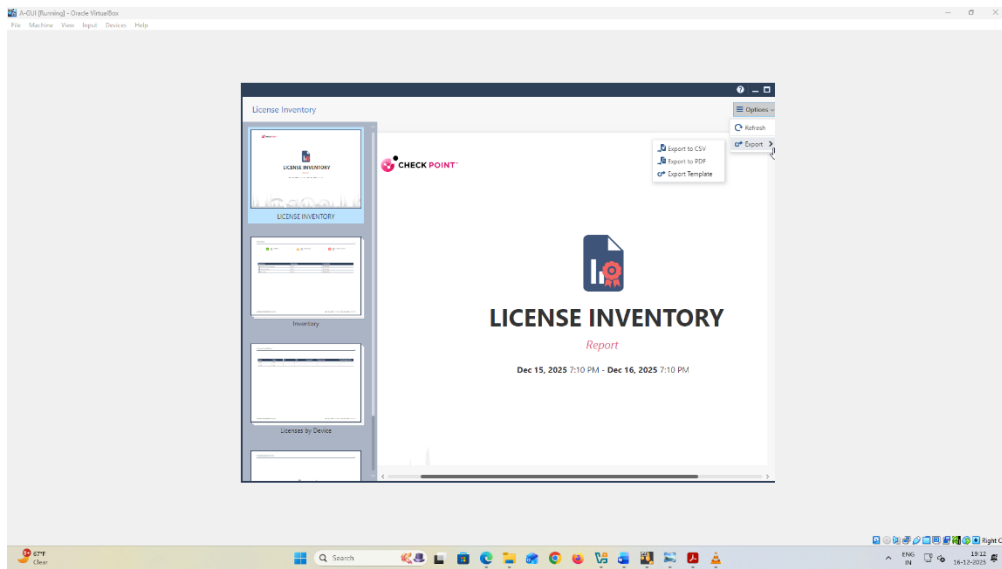


Figure 19: License Inventory Report Export Options Menu

3. FIREWALL POLICY IMPLEMENTATION AND TRAFFIC CONTROL

3.1 Enterprise Security Policy Framework

The enterprise security policy framework is considered to limit unauthorized inbound and outbound flows and ensure that necessary business continuity exists between the two site enterprise environment. It is interested in bridging an operational requirement to access core enterprise services and administrative access control into enforceable operating firewall rules which are explicitly justified and provable. The framework has also taken into account the additional control of facilitating additional controls, including IPS, anti-malware, and user authentication or identity awareness to enable more granular and role-conscious enforcement to the extent implemented. Any policy decision made is vindicated in contrast to the expectations of real-life enterprise security and positioned as an improvement consonant to the accepted industry standards [7], [8], [9], [10], [11], as mandated by the brief to make the network more secure with the aid of Gaia appliances and formal Check Point instructions.

3.2 Firewall Rule Base Design and Architecture

Security access Security is managed with the help of SmartConsole Security Policies view, using the rule base that forms a structured way of governing the traffic. The ordering of rules is based upon the rule of placing the most specific rules first then more general, so that more specific conditions of match are checked in the first place and less specific conditions should only be invoked when more specific ones have been violated. Such a top to bottom assessment rationale ensures that rules that are too lenient are not accidentally enabling traffic that would be denied by a stricter set of policies.

A final deny-all rule placed at the base of the rule base provides a default deny rule which drops any traffic not explicitly allowed by rules which precede the deny-all rule, which is a secure-by-default posture that

mirrors the principle of least privilege. There are screenshots of the overall rule base structure, which show the logical flow of particular denials and allowances, up to the ultimate implicit drop.

Implementing stealth rules guard the gateway interface, not allowing it to pass traffic directly to interfaces services managing or monitoring explicitly popular services; in this way, the attacker attempts that the security infrastructure will be reconnoitered, and direct attacks made. End of policy cleanup rule configuration also maintains sensible logging and processing of the traffic that is not covered by any explicit rule to support visibility of the blocked connection attempts in the security check and the policy optimization.

Network objects are built in SmartConsole to represent logical groupings before the rules are built. SwanseaNetwork object corresponds to 192.168.1.0/24, which corresponds to the enterprise topology laid out in Part 1, LondonNetwork corresponds to 192.168.2.0/24 and Management Network corresponds to 10.1.1.0/24. The screenshots of the object database indicate systematized organization of the database as a way of managing policies effectively.

Critical servers such as S-DC at 192.168.1.1 (Primary Domain Controller SWANSEA.ACCA), L-CD at 192.168.2.1 (Child Domain Controller LONDON.SWANSEA.ACCA) and other IIS web servers implemented within the environment can have host objects created. These items allow fragmentary access to vital infrastructure services to be controlled.

3.3 Inbound Traffic Rules Configuration

3.3.1 ICMP Traffic Control

The inbound ICMP rule is configured with source set of Any (representing the sources in the Internet), destination set of internal networks (between swansea networks and London networks objects), and service set of icmp-proto which includes ego-request packets. The move will be to Drop and allow logging on, preventing external ping sweeps and reconnaissance of the network topology and active hosts to potential attackers. This avoids information disclosure and preservation of perimeter security. Exceptions can be added to do diagnostic work, so ICMP of ManagementNetwork could be used to legitimate internal destinations to do thorough troubleshooting by responsible administrators.

3.3.2 HTTP/HTTPS Web Traffic Rules

Part 1 allow Rule to permit Inbound web traffic to DMZ-hosted web servers The rule should be configured with a source value of Any, a destination value of WebServerObject (which indicates Web Server of Part 1) and services of both http (TCP port 80) and https (TCP port 443), action Accept and Track equals to Log to generate audit trails. When the gateway is positioned in front of web servers, NAT settings would be translated to the IP addresses of the internal server to facilitate access by a person outside and the internal server network to avoid exposition of internal addressing plans.

3.3.3 SSH Remote Administration Control

The remote administration is limited to SSH access through configuration of source as ManagementNetwork or specific administrator host objects, destination as the internal servers that are required to be managed, service ssh (TCP port 22) and action Accept. This rationale indicates that confinement of administrative access to trusted areas within management has a profound reduction in the attack surface due to blocking any attempts of unauthorized connections of SSH by the untrusted networks, and this is in line with least privilege.

3.3.4 FTP Service Restrictions

A rule that blocks FTP traffic has the following settings; source Any and destination to internal networks, services ftp (TCP port 21) ftp-data (TCP port 20) and action drop. Security justification is that FTP uses cleartext to transmit credentials and data and as a result they can be intercepted. Encrypted file transfer can be delivered through modern secure implementations like SFTP (SSH File transfer protocol) or FTPS (FTP over SSL/TLS), and is recommended.

3.3.5 Telnet Protocol Blocking

Action Drop and deny telnet traffic s Dennis (TCP port 23). Reason is that Telnet sends all the information including authentication data in plaintext format without encryption, illness of revealing sensitive information to network eavesdropping. SSH has supplanted Technet as the obligatory utilization of safe distant command-line access.

3.4 Outbound Traffic Rules Configuration

3.4.1 Internet Access for Internal Users

A rule is executed with a source set of InternalNetworks (SwanseaNetworks object + LondonNetworks object), a destination set of Any or Internet object, and with a services set of http (TCP 80) and https (TCP 443) and dns (UDP 53) services and action Accept with logging which permits outbound web browsing. It is an opportunity to use legitimate internet access by business internal users without loss of visibility by tracking logs. Application-level filtering can be applied to this rule where Application Control blade is enabled as an enhanced feature to allow only certain web applications such as social media or file sharing service to be permitted instead of simple port-level regulation. In case Identity Awareness is enacted, group or user objects can be configured as source to differentiate the policies of internet accesses regarding role of users so that administrators can have greater access than ordinary users.

3.4.2 Email and Communication Services

Email traffic policy has been established at SMTP (TCP 25), POP3 (TCP 110) and IMAP (TCP 143/993) and has been set to only allow access to internal mail server objects and any destination to the Internet with action being Accept. Avoiding the use of workstations across the entire domain for email relaying by sources and

allowing only specific mail servers to do so will avoid using compromised workstations to relay spam or steal data through unauthorized email gateways, therefore controlling email gateway architecture.

3.4.3 Outbound Administrative Traffic

Other rules are configured with a source restriction to ManagementNetwork or specific administrator hosts, a destination restriction of Any and an action of accept with extensive logging policy. Outsourcing the sources of administrative protocols will allow only the legitimate managed administrative workstations to form outbound administrative links and help minimize the risk of credential theft and horizontal mobility. Security monitoring and incident investigation Make audit trails of security monitoring and incident investigation purposes available via logging requirements.

3.5 Inter-Site VPN Traffic Rules

A site to site VPN rule is tested to allow encrypted communication between the two locations of the enterprise that was set in Part 1. The rule is as follows; source SwanseaNetwork (192.168.1.0/24) and the destination LondonNetwork (192.168.2.0/24), VPN column = the current S2S VPN community object and action = Accept. The encryption domain is verified to ascertain that both ranges of networks are enclosed in VPN tunnel configuration that will assure that traffic between sites are automatically encrypted when it is passing through the outside link.

The reason why inter-site communications have to be encrypted is as follows: the communications between the domains of SWANSEA.ACCA and the LONDON.SWANSEA.ACCA are supposed to be transferred over potentially insecure networks and confidentiality and integrity should be guaranteed. The VPN provides a security measure against the eavesdropping and alteration of sensitive internal information by others such as Active Directory replication, user authentication traffic, and files sharing information between sites.

4. ENHANCED SECURITY FEATURES IMPLEMENTATION

4.1 Proposed Additional Security Enhancements

The assessment brief suggests adding more security capabilities with the help of Gaia appliances based on the recognised industry standards and usage of official guidelines of Check Point to provide more strength to the enterprise network. Through a risk-based prioritisation method, controls that reduce such typical enterprise threats are identified and are mapped to known attacker approaches [12] and web application risks with references to frameworks like MITRE ATT&CK and OWASP [13], [14]. IPS is given first priority in order to minimize exposure to network and protocol exploitations [15], [16]. Applications Control and URL Filtering is the one that is chosen to address web risk outside port-based rules, and to apply the acceptable-use controls. To facilitate role-based enforcement, Identity Awareness and user-based access control are also present to be used as one of the added features pointed out in the brief. Anti-Malware and Anti-Bot security is chosen to minimize malware intrusion and command and control.

These features add both content, application and identity context to firewall rules and demand performance, operational overhead and user experience impact to be handled employing specific profiles, progressive enablement and accurate scope of the rule.

4.2 Intrusion Prevention System (IPS) Configuration

4.2.1 IPS Profile Creation and Assignment

Operation of IPS blade is achieved by visiting the properties of A-GW gateway objects in the SmartConsole and navigating to the tab of Software Blades. The option of intrusion prevention system is IPS which is activated together with Firewall blade. An IPS profile is chosen, which can be Optimized; to achieve the maximum security and possible performance loss Strict; Strict, or Custom; to achieve a protection profile chosen obviously depending in our particular organizational needs.

The signature database updates are set to make sure that the latest threat intelligence and attack signatures are delivered to the gateway automatically by Check Point update services which usually need valid service contracts. The types of attack protection are turned on to prevent several types of threats: Network attacks to prevent reconnaissance, scanning, and exploits at the network layer; Application intelligence to prevent application and service-specific attacks and Protocol anomaly detection to identify traffic that does not adhere to the RFC standards or has suspicious deviations to the typical protocol behavior, including zero-day exploits and evasion strategies.

4.2.2 IPS Rule Integration

IPS inspection is seen to complement firewall rules by modifying existing Accept rules and only adding IPS to the inspection setting column. Inline mode proactively blocks the threats that are detected in real time whereas detect only mode logs the threats and does not block them which can be used during initial tuning stages. Exception management gives administrators the power to make known false positives a bypass rule without having to sacrifice the overall protection effectiveness.

4.3 Application Control and URL Filtering

The A-GW gateway has Application Control enabled that allows the identification of traffic as well as the control of traffic based on the applications it carries and not just the ports. The policy establishes a set of categories to block social media and file sharing of a person paying attention to permission of adequate productivity and collaboration applications required to conduct business activities. Organisation specific tools could have custom application rules that are created.

URL Filtering is turned on to control web browsing according to the categories and prevent the entry of known malicious sites, adult material and other categories regarded as biased to the business by the company, and thus minimise the possibility of infection and data leaking through the user.

4.4 Identity Awareness and User-Based Access Control

To further ensure a higher level of security which was noted in the brief, Identity Awareness is also turned on in A-GW such that access decisions are made based on authenticated user groups and not just IP addresses. Integration uses the existing environment of Active Directory by utilizing the use of the primary domain controller S-DC in 192.168.1.1 and applying the obtained identity mappings to enforce on a user basis. AD groups are depicted as Administrators, StandardUsers and limited access users, and employed by firewall rules to permit administrative access to Administrators only, control the management of the web server to authorised groups only, and introduce differentiated internet access policies with logging to protect accountability.

4.5 Anti-Malware and Anti-Bot Protection

In the assessment, it is indicated that enabling the anti-malware protection is a bonus when implementing the enterprise firewall policy. In this context, the Threat Prevention settings are to be recorded on the gateway and implemented on pertinent traffic regulations and the time-stamped images to be provided as a witness in the report. The brief does not state what Anti-Bot settings, protocol specific inspection requirements, and file type filtering requirements are so these may only be stated where they can be established as configured and seen in the implementation.

5. TESTING, VALIDATION, AND OPERATIONAL VERIFICATION

5.1 Connectivity Testing

After installation of Check Point infrastructure, connection between A-SMS and A-GW is checked by ensuring that SIC status shows "Communicating" in the gateway properties Communication settings. The connection of SmartConsole to the network is tested successfully due to the ability to enter 10.1.1.101 through A-GUI and execute all management capabilities without exceptions. All appliances are checked on the Gaia web portal or via the command line using interface status, which ensures that in all A-GW both eth0, eth1, eth2 and eth3 all are live and correctly configured in terms of link status and IP address assignments. Verification of routing table A-GW: checks with routing table are done to verify that routes to SwanseaNetwork, LondonNetwork, and external networks are configured up to courses of directing traffic via relevant interfaces. There is evidence of ping tests between A-GUI to A-SMS (10.1.1.101) and between A-GW (10.1.1.1) and successful replies displaying this layer 3 connectivity with the traceroute showing path verification all with visible timestamps which are visible as needed to submit reports to the report receiver.

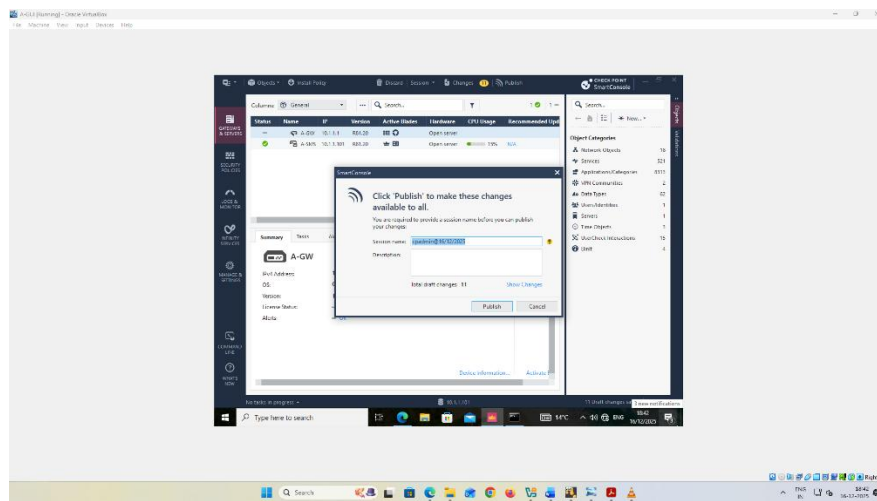


Figure 20: Publish Session Dialog with Draft Changes

5.2 Firewall Rule Testing Methodology

Authorized traffic is authenticated by attempting the (HTTP and HTTPS) connections between client machines internal (ClientS1 or ClientL1) and web servers or other target in the internet by checking whether they can successfully connect. Connectivity to the SSH of Management_Network hosts to internal servers is verified and the success of authorized administrative access is ensured. Blocked traffic verification involves checking external ICMP echo to internal host, confirming drops, checking FTP and Telnet connections and logging denial and trying SSHs using unauthorized source networks to confirm denial. SmartConsole Logs & Monitor view is used to see the traffic logs in real time and screenshots display the accepted and dropped connections with references to a fixed number of rules and prove the effectiveness of the policy and the right order of rules evaluation.

5.3 Enhanced Security Feature Validation

When applied as part of IPS, Application Control, Identity Awareness, or Anti-Malware extensions, the validation evidence is logged in the SmartView Tracker security events of detections, blocks, user authentication confirmation, etc, which can be used to support the demonstration requirement.

6. CONCLUSION AND SECURITY POSTURE ASSESSMENT

6.1 Implementation Summary

This has been implemented effectively to secure the enterprise network by ensuring that all the three requirements of Part 2 of the assessment are fulfilled. To begin with, the Check Point Security Management Server, Security Gateway and SmartConsole were installed with the corresponding licensing, which created the central policy management/monitoring functions throughout the SWANSEA.ACCA and LONDON.SWANSEA.ACCA environment. Second, with respect to a real-life enterprise security policy framework to fit in with the needs of the operational requirement of the two-site topology, justified firewall rules were created and enforced, including controls on ICMP, HTTP/HTTPS, SSH, FTP, and Telnet. Third,

other security functionalities were suggested and developed with the use of Gaia appliances, proving to have better security as per the industry standards and official Check Point directions. This has enhanced the security posture with defense in depth [17] through basic drafts to liescent inspection, policy-based enforcement, and centralized visibility [9], [11]. It has been connected to existing Active Directory infrastructure without affecting business continuity but with added security control.

6.2 Operational Considerations and Future Enhancements

Constant control means that policy changes are necessary to keep up with business requirements, signature and blade modifications that are needed to sustain protection of current threats, constant monitoring with SmartConsole Logs and Monitor in order to notice the presence of anomalies and breaches of the policies. To improve further, automation of security, particularly how incident response is handled, the addition of better quality threat intelligence feeds so that an organization can actively defend against attacks, and a security orchestration component to structure responses across a number of security layers could become part of the list. The career maturity and advancement in the cybersecurity roles will be facilitated by professional growth in Check Point administration and the overall practice of security management.

7. REFERENCES

- [1] NIST, “The NIST cybersecurity framework (CSF) 2.0,” *NIST Cybersecurity Framework. CSF 20*, vol. 2.0, no. 29, 2024, doi: [10.6028/nist.cswp.29](https://doi.org/10.6028/nist.cswp.29).
- [2] “Framework 2.0: RESOURCE & OVERVIEW GUIDE,” 2024, doi: [10.6028/NIST.SP.1299](https://doi.org/10.6028/NIST.SP.1299).
- [3] “What is the NIST Cybersecurity Framework 2.0?,” Rubrik. [Online]. Available: <https://www.rubrik.com/insights/nist-framework-explained>
- [4] T. Olaes, “What is the NIST Cybersecurity Framework?,” Balbix. [Online]. Available: <https://www.balbix.com/insights/nist-cybersecurity-framework/>
- [5] “GAIA R81.20 Administration Guide,” 2025. [Online]. Available: https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_Gaia_AdminGuide/CP_R81.20_Gaia_AdminGuide.pdf
- [6] CheckPoint, “QUANTUM SECURITY MANAGEMENT | R81 | Administration Guide,” checkpoint. [Online]. Available: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/CP_R81_Quantum_SecurityManagement_AdminGuide.pdf
- [7] R. HARPER, “ISO 27001: 2022 Update -Everything You Need to Know- ISMS.online,” <https://www.isms.online/>. [Online]. Available: <https://www.isms.online/information-security/everything-you-need-to-know-about-the-iso-27001-2022-standard-update/>
- [8] “ISO/IEC 27001 Information Security Management System | NSAI,” NSAI. [Online]. Available: <https://www.nsai.ie/certification/management-systems/iso-iec-27001-information-security-management-system/>
- [9] International Organization for Standardization, “ISO/IEC 27001 standard – information security management systems,” ISO. [Online]. Available: <https://www.iso.org/standard/27001>
- [10] A. Schirn, “ISO/IEC 27001:2022 – Information Security Systems - ANSI Blog,” The ANSI Blog. [Online]. Available: <https://blog.ansi.org/anab/iso-iec-27001-2022-information-security-systems/>
- [11] “ISO/IEC 27001:2022/Amd 1:2024,” ISO. [Online]. Available: <https://www.iso.org/standard/88435.html>
- [12] MITRE ATT&CK, “Matrix - Enterprise | MITRE ATT&CK™,” [attack.mitre.org](https://attack.mitre.org/matrices/enterprise/). [Online]. Available: <https://attack.mitre.org/matrices/enterprise/>
- [13] Joint Task Force, “Security and Privacy Controls for Information Systems and Organizations,” *Secur. Priv. Controls Inf. Syst. Organ.*, vol. 5, no. 5, 2020, doi: [10.6028/nist.sp.800-53r5](https://doi.org/10.6028/nist.sp.800-53r5).
- [14] NIST, “Security and Privacy Controls for Information Systems and Organizations,” [csrc.nist.gov](https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final). [Online]. Available: <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>
- [15] Center for Internet Security, “CIS Controls Version 8,” CIS. [Online]. Available: <https://www.cisecurity.org/controls/v8>
- [16] “CIS Critical Security Controls Version 8.1,” CIS. [Online]. Available: <https://www.cisecurity.org/controls/v8-1>
- [17] A. Z. Mahfud, I. R. Hikmah, Septia Ulfa Sunaringtyas, and Tiyas Yulita, “Information Security Risk Management Design Based on ISO/IEC 27005:2022, ISO/IEC 27001:2022, and NIST SP 800-53 Revision 5 (A Case Study at ABC Agency),” pp. 181–186, 2024, doi: [10.1109/ice3is62977.2024.10775428](https://doi.org/10.1109/ice3is62977.2024.10775428).