

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

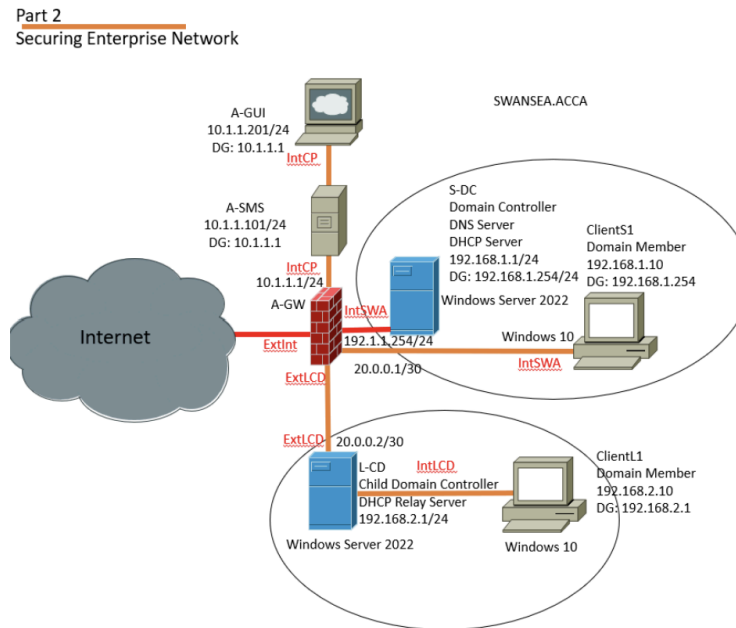
Name: Jyothi Avulareddygar
MSc (Cybersecurity and Digital Forensics)
Enterprise Network Security
Module code: ACCA7032

Table of Content

Introduction.....	3
Installation and Configuration of Lab.....	4
Firewall Rules Configuration and Policy Implementation.....	23
Firewall Rules Configuration and Enterprise Security Policy Implementation.....	23
ICMP Configuration.....	24
FTP Configuration.....	25
SSH Access Rule.....	26
Validating the policy.....	27
Enhanced Security Implementation Through Advanced Features.....	29

Introduction

Overview of the Enterprise Network



The network in question is part of a blend model, combining a traditional Windows infrastructure with a dedicated systems security system (Check Point). As shown in the topology, the environment is divided into two main areas, SWANSEA.ACCA and LONDON.SWANSEA.ACCA. A dedicated point to point connection over the 20.0.0.0/30 subnet connects these sites, creating a WAN backbone through which seamless communications and sharing of resources between the sites can occur throughout the organization.

At the heart of the network is the SWANSEA.ACCA site which works as the center core and main administrative domain. This site is anchored by the root Active Directory Domain Controller known as S -DC, and with the IP address 192.168.1.1/24. This controller has several important functions, including DNS resolution, DHCP services, centralized identity and policy (Active Directory). A client workstation called ClientS1, with the address value of 192.168.1.10, is in this subnet, a member of the domain. The LONDON.SWANSEA.ACCA site, on the other hand, is a child domain. It contains an additional domain controller, L-CD at 192.168.2.1/24 that is configured as a relay agent for the Domain Name System (DNS) and has its own client workstation, Client11 (192.168.2.10).

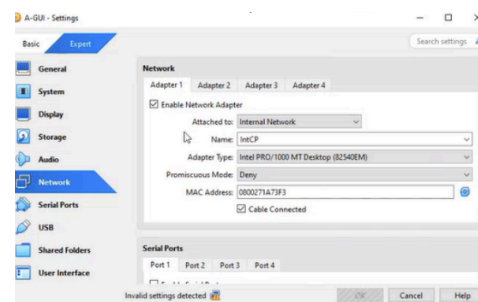
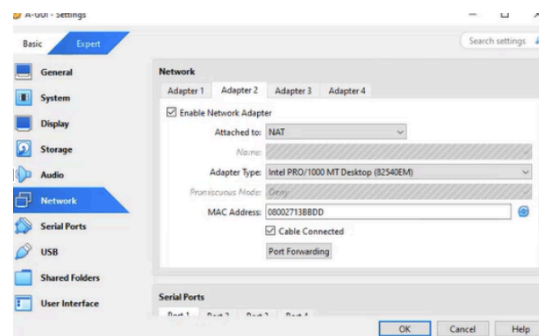
A defining characteristic of this architecture is the introduction of a Check Point security suite which is deployed in its own segregated management network (10.1.1.0/24). This suite is

constructed around three major appliances. The security management server (A-SMS at 10.1.1.101) is the central nervous system that contains the master security policy and acts as the administrative command center. Directing and checking the traffic is the Security Gateway (A-GW), at a strategic position being the default gateway (192.168.1.254) for the Swansea local network. Administration is done from the dedicated Graphical User Interface workstation (A-GUI, 10.1.1.201) where the Smart Console application is run. This whole setup creates an effective hub-and-spoke model of security, where any traffic containing your protected internal networks (travelling to or from) will first have to pass through the security gateway where it will undergo thorough application of policy and threat analysis.

Installation and Configuration of Lab

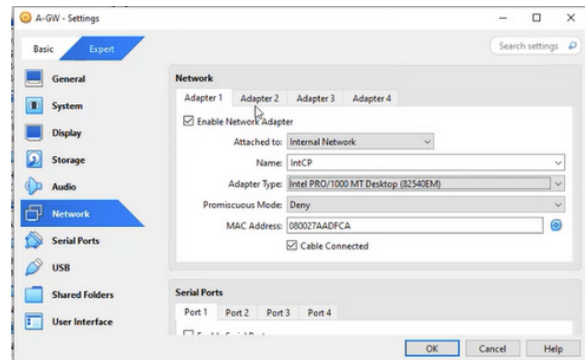
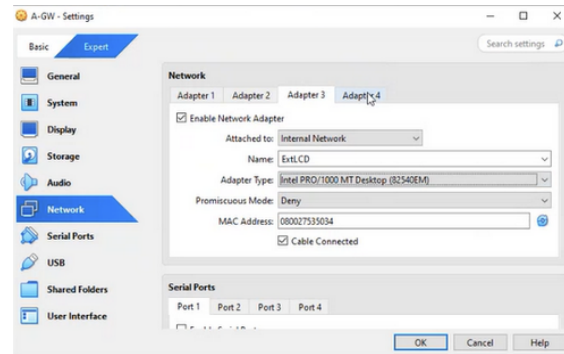
Configuring Network Settings

The laboratory environment for Check Point is architected on a precise strategy of network segmentation using Oracle VirtualBox. A principal part of this strategy involves the use of a separate internal network switch designated "IntCP" which is solely used for management traffic. This switch is used to provide the connection between the Administrative GUI workstation (A-GUI), the Security Management Server (A-SMS), and the Security Gateway (A-GW). The intent behind this segregated network is to provide a secure and reliable path of communications for sensitive administrative functions, such as distribution of policies and aggregation of logs, effectively segregating this (control plane) from the data streams for users. For operational needs for external connectivity, additional network interfaces configured via NAT mode are provided for the A-GUI and A-SMS appliances. This implementation allows for required outbound connectivity to the internet for contents such as license checking and threat database updates, this is done via the network stack on the hosting machine without compromising the security



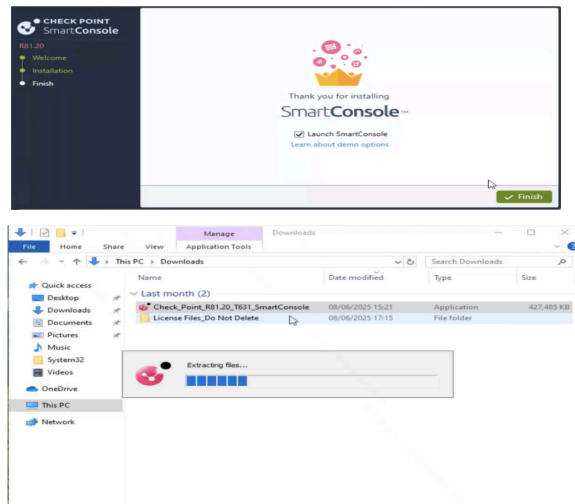
wall between the segments forming the internal lab.

The Security Gateway (A-GW) is the main instrument used for policy enforcement in the architecture, and uses a multi-homed interface configuration which mimics a production enterprise topology. In addition to having a dedicated management interface located on the "IntCP" network segment, the gateway platform has three functionally different network adapters. The first adapter is configured for Network Address Translation (NAT) which emulates the untrusted external internet connection. The second adapter has connectivity to the "IntSwa" internal network, for the Swansea headquarters local area network. The third adapter provides a connection to the "ExtLCD" network, which is a simulated connection to the wide-area network (WAN) interconnection to the remote London branch facility. This exact logical segmentation across four independent interfaces allows for the definition and consistent enforcement of security policy between the management domain, the internal corporate network, the remote site network and a simulated internet perimeter.



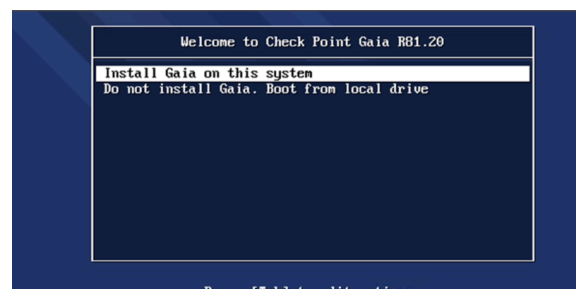
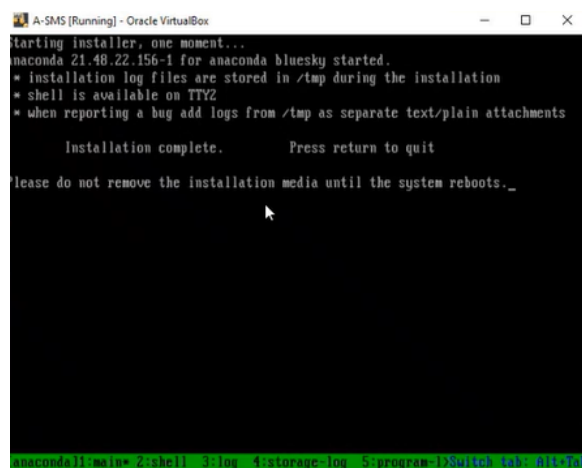
Installation of SmartConsole on A-GUI

Documented by screenshots, the process of installing the Check Point SmartConsole is a clear linear process on the A-GUI workstation. It starts with the installer starting in the Downloads directory. The first step is file extraction (indicates extraction in a progress bar), then a setup status screen indicates completion of 15% but also enjoys the promotional tagline "Efficient Automated Operations." The process ends with the success confirmation for SmartConsole R81.20. This completes the deployment, and the administrator should be able to start using the client for centralized control and monitoring of the security infrastructure.

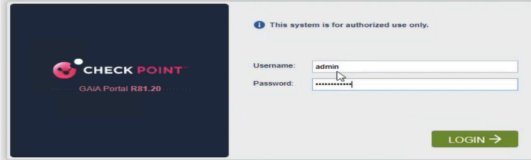


Installing the Primary Security Management Server (A-SMS)

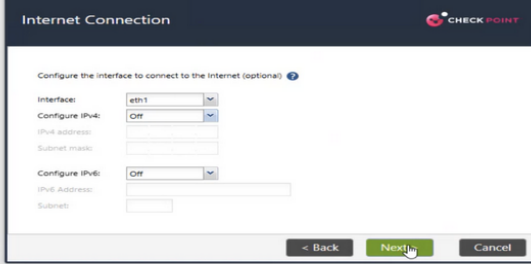
The Check Point Security Management Server (A-SMS) deployment procedure is invoked by booting the appliance using the Gaia R81.20 installation media. The starting point is to carve up the local 80GB storage device based on the default template where specific amounts of space are allocated for root file system, logging data, swap space and reserved capacity for further backups or software upgrades. The operating system files are then copied on the configured partitions. This installation stage is formally completed with a confirmation prompt which requires a system reboot to complete the execution of the installation and initializing the newly installed Gaia operating environment.



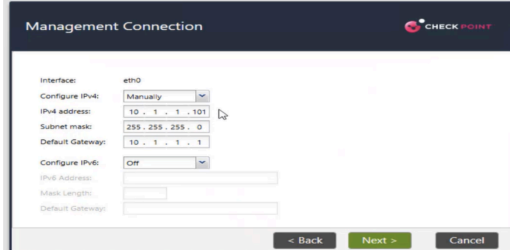
Post-reboot, a browser is opened to the A-GUI client and from there administrative access is gained to the Gaia Portal, where the First Time Configuration Wizard is executed first. A very important configuration task of this wizard is a manual declaration of the parameters of the main management network interface (eth0). The Static IP Address - 10.1.1.101, Subnet Mask - 255.255.255.0 and Default Gateway - 10.1.1.1 are assigned to align the server with the predefined security management network segment of the lab environment. This initial network setting up accommodates basic level 3 connectivity for a management server to communicate with the graphene control plane as well as provides a platform for some set up operations to take place later down the line for this platform.



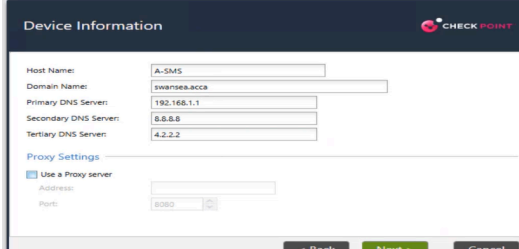
The login screen for the Check Point Gaia Portal R81.20. It features the Check Point logo on the left and a login form on the right. The form includes fields for Username (admin) and Password (masked with dots), and a LOGIN button.



The Internet Connection configuration screen. It prompts the user to "Configure the interface to connect to the Internet (optional)". The interface is set to eth1. The "Configure IPv4" dropdown is set to "Off". There are fields for IPv4 address, Subnet mask, and Default Gateway, all of which are empty. The "Configure IPv6" dropdown is also set to "Off". At the bottom, there are buttons for "< Back", "Next >", and "Cancel".



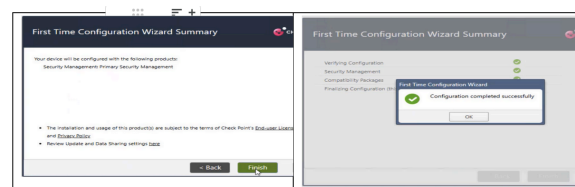
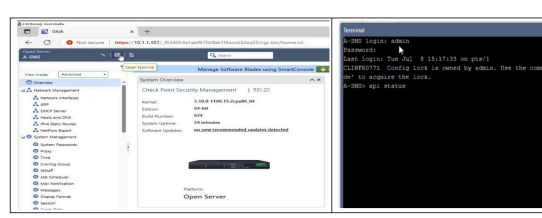
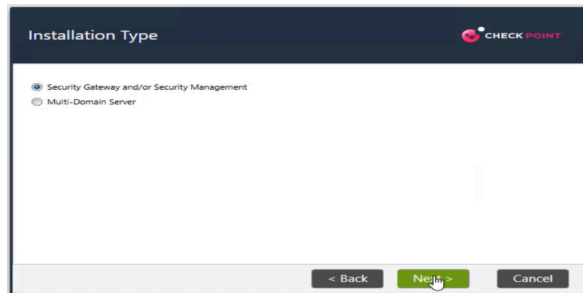
The Management Connection configuration screen. It prompts the user to "Configure the interface to connect to the management network". The interface is set to eth0. The "Configure IPv4" dropdown is set to "Manually". The IPv4 address is set to 10.1.1.101, the Subnet mask is 255.255.255.0, and the Default Gateway is 10.1.1.1. The "Configure IPv6" dropdown is set to "Off". There are fields for IPv6 Address, Mask Length, and Default Gateway, all of which are empty. At the bottom, there are buttons for "< Back", "Next >", and "Cancel".



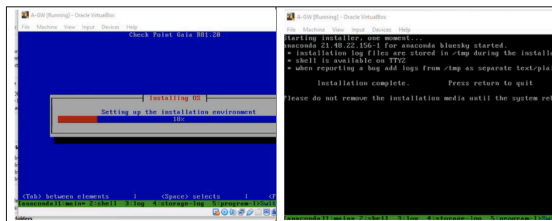
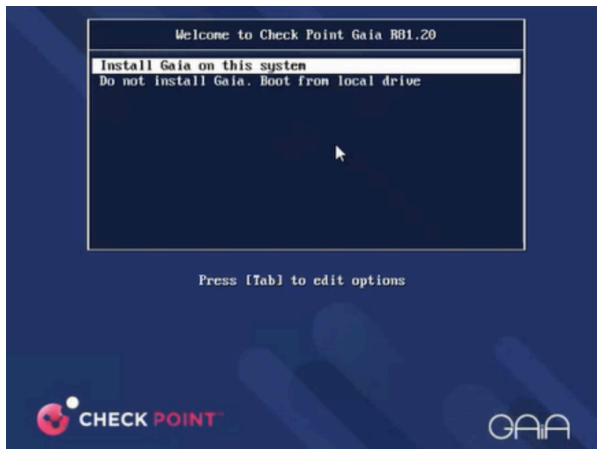
The Device Information configuration screen. It prompts the user to "Configure the device information". The fields are: Host Name (A-SMS), Domain Name (swansea.acca), Primary DNS Server (192.168.1.1), Secondary DNS Server (8.8.8.8), and Tertiary DNS Server (4.2.2.2). There is a section for Proxy Settings with a checkbox "Use a Proxy server" which is unchecked, and fields for Address and Port (8080). At the bottom, there are buttons for "< Back", "Next >", and "Cancel".

The First Time Configuration Wizard moves on to the phase where the fundamental identity and operational profile for the Security Management Server appliance is being defined. Configuration parameters such as the mapping of the host-name "A-SMS" and membership of the "swansea.acca" domain. Network name resolution setup using a primary DNS server together with an internal Domain Controller (Zhi Xiang 192.168.1.1) is set up for easy access to internal resources, with secondary external DNS servers (for redundancy and access to external services). The deployment profile is explicitly set to "Security Gateway and/or Security Management," which again is in line with a standard organizational deployment model and avoids the Multi-Domain Server mode which is for managed service providers.

Later configuration is made for administrative security policy. Access control lists have been defined to only allow management connections from the 10.1.1.0/24 ip address range: this will only allow management connections from designated management work stations on that segment. The wizard ends with a final summary with the appliance initialized as a "Primary Security Management" server. Post configuration verification is performed using the Gaia Web UI interface and the System Overview verifies the status of the R81.20 platform, followed by a CLI command that verifies the operational readiness of the management API service.



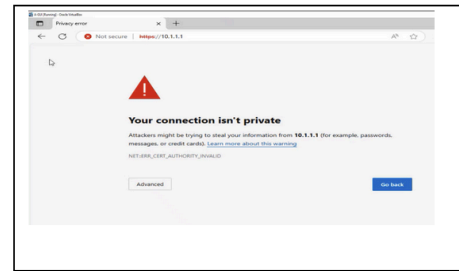
Installation of the Check Point Gateway (A-GW)



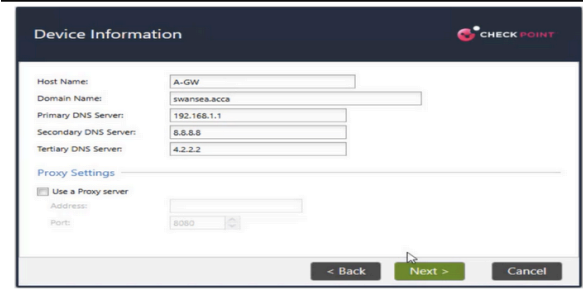
Deployment Procedure for the Security Gateway (A-GW) is started by booting the virtual appliance from the Check Point Gaia R81.20 installation media. The mode of operation is determined by selecting the "Install Gaia on this system" option on the presented start-up menu, which initiates the installation of the operating system. The process runs an automated setup sequence, the completion status of which is specified by a graphical progress indicator. The installation cycle ends with a confirmation dialogue that has the message "Installation complete." A manual reboot is then needed, which is triggered with a keystroke, to complete platform initial setup for the gateway appliance.

Running the First Time Wizard on the Security Gateway

The initial configuration of the Security Gateway (A-GW) appliance is done via access to the Gaia WebUI in the management client. Administrative access begins by bypassing the browser security warning for the self-signed certificate to the authentication interface. Execution of the First Time Configuration Wizard results in validation of the primary management network interface (eth0), which is pre-configured to have a static address 10.1.1.1/24 for the purpose of assurance of layer 3 connectivity within the management plane. Configuration of the secondary interface (eth1) is postponed here and both IPv4 and IPv6 address configuration remains inactive.

A screenshot of the 'Management Connection' configuration page in the Check Point Gaia WebUI. The page has a dark header with the Check Point logo. The main content area is white and contains configuration fields for the 'eth0' interface. Fields include 'Interface' (eth0), 'Configure IPv4' (Manually), 'IPv4 address' (10.1.1.1), 'Subnet mask' (255.255.255.0), and 'Default Gateway' (-.-.-). There are also fields for 'Configure IPv6' (Off), 'IPv6 Address', 'Mask Length', and 'Default Gateway'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.A screenshot of the login page in the Check Point Gaia WebUI. The page has a dark header with the Check Point logo and 'Gaia Portal R81.20'. On the right, there is a login form with fields for 'Username' (admin) and 'Password' (masked with asterisks). Below the fields is a green 'LOGIN >' button. A message at the top right says 'This system is for authorized use only.'A screenshot of the 'Internet Connection' configuration page in the Check Point Gaia WebUI. The page has a dark header with the Check Point logo. The main content area is white and contains configuration fields for the 'eth1' interface. Fields include 'Interface' (eth1), 'Configure IPv4' (Off), 'IPv4 address', 'Subnet mask', 'Configure IPv6' (Off), 'IPv6 Address', and 'Subnet'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

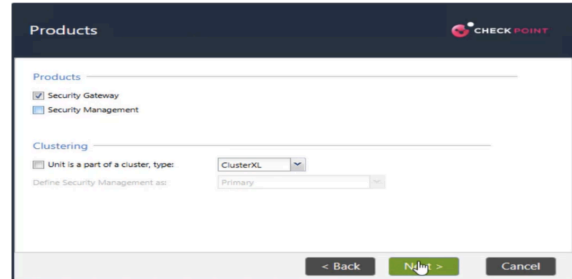
Following configuration steps are used to provide the identity of the device, including the hostname (A-GW) and domain membership (swansea.acca). Access to Domain Name System (DNS) resolution is set up using the internal Domain Controller (192.168.1.1) as the primary one and outside resolvers as the secondary redundancy. The wizard then defines the functional profile with choice "Security Gateway" product role with explicit de-selection of "Security Management" capability, i.e. characterizing the appliance as a dedicated policy enforcement point. Clustering functionality is still disabled, and the device is set apart for static IP addressing. The procedure concludes with the establishment of the Secure Internal Communication (SIC); the administrator enters the pre-shared activation key Chkp!234 in order to prime the trusted communication channel that is required between the Security Management Server to manage this gateway node.



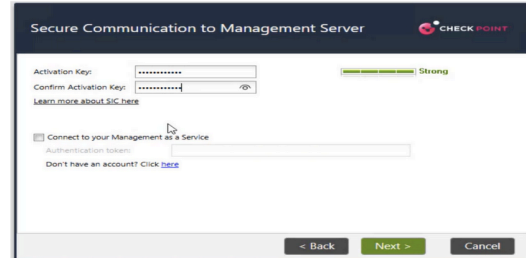
The "Device Information" screen in the Check Point wizard. It contains fields for Host Name (A-GW), Domain Name (swansea.acca), Primary DNS Server (192.168.1.1), Secondary DNS Server (8.8.8.8), and Tertiary DNS Server (4.2.2.2). Below these is the "Proxy Settings" section with a checkbox for "Use a Proxy server" and fields for Address and Port (8080). Navigation buttons at the bottom are "< Back", "Next >", and "Cancel".



The "Dynamically Assigned IP" screen. It asks "Does this gateway have a dynamically assigned IP address (DAIP gateway)?" with radio buttons for "Yes" and "No". The "No" option is selected. Navigation buttons at the bottom are "< Back", "Next >", and "Cancel".



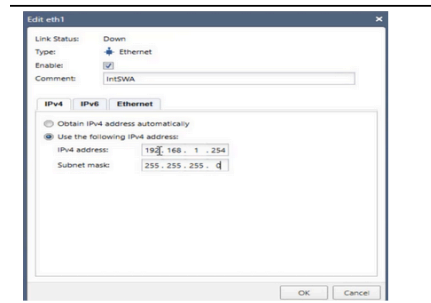
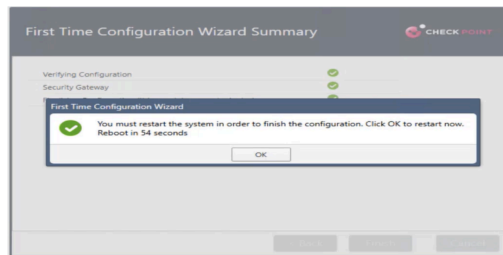
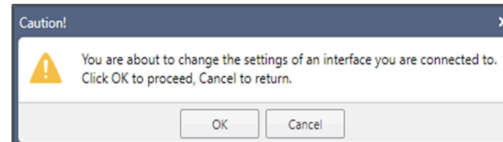
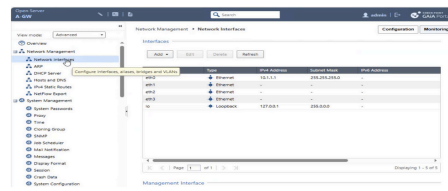
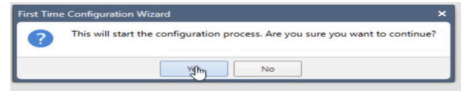
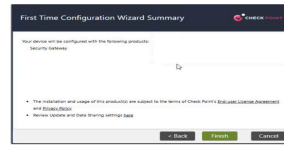
The "Products" screen. It shows "Products" with checkboxes for "Security Gateway" (checked) and "Security Management" (unchecked). Below is the "Clustering" section with a checkbox for "Unit is a part of a cluster, type:" set to "ClusterXL" and "Define Security Management as:" set to "Primary". Navigation buttons at the bottom are "< Back", "Next >", and "Cancel".



The "Secure Communication to Management Server" screen. It has fields for "Activation Key:" and "Confirm Activation Key:" both containing "*****". A strength indicator shows "Strong". There is a link "Learn more about SIC here". Below is a checkbox for "Connect to your Management as a Service" with an "Authentication token:" field. A link "Don't have an account? Click here" is present. Navigation buttons at the bottom are "< Back", "Next >", and "Cancel".

The process of initial configuration of the Security Gateway (A-GW) appliance concludes with a review and confirmation phase for the First Time Configuration Wizard. The administrator checks if the defined product role is set to "Security Gateway" and makes the finalization by clicking "Finish," thereby committing all the parameters that were configured. A mandatory system reboot is performed to load up and activate the new software identity and network stack.

Following the rebooting, the administrative access is re-established through the Gaia Portal to make final provisioning of the network. Inside the Network Management interface the main management interface eth0 is verified to be running with the static assigned address 10.1.1.1. Subsequently, the internal facing interface (eth1) is administered and has the static IP address of 192.168.1.254. An interface comment field is filled with the value "IntSWA" so that it will be known that this logical link is to the Swansea internal corporate network segment.



The final part of the Security Gateway (A-GW) network configuration is the provisioning of the final two physical interfaces. The administrator starts setting up configuration on interface eth2 and enables the port administratively and assigns the interface comment "ExtLCD." A static address of 20.0.0.1 on the IPv4 address is provided with a subnet mask of 255.255.255.252: define this interface as the link to the London segment, that is, a point-to-point routed link. After that, interface eth3 is configured: the interface is enabled, is labeled "ExtInt" via the comment field, and has IPv4 addressing mode set to dynamic (DHCP client) because this is used as the external perimeter interface. Upon application of aforementioned parameter changes, the administrative session is ended after logging out of Gaia WebUI and closing the browser client and finalizing the interface configuration task.

Interfaces

Add Edit Delete Refresh

Name	Type	IPv4 Address	Subnet Mask	IPv6 Address
eth0	Ethernet	10.1.1.1	255.255.255.0	-
eth1	Ethernet	192.168.1.254	255.255.255.0	-
eth2	Ethernet	20.0.0.1	255.255.255.252	-
eth3	Ethernet	-	-	-
lo	Loopback	127.0.0.1	255.0.0.0	-

Page 1 of 1

Displaying 1 - 5 of 5



Edit eth3

Link Status: Down

Type: Ethernet

Enable: ☒

Comment: ExtInt

IPv4 IPv6 Ethernet

☒ Obtain IPv4 address automatically

☐ Use the following IPv4 address:

IPv4 address:

Subnet mask:

OK Cancel

Edit eth2

Link Status: Down

Type: Ethernet

Enable: ☒

Comment: ExtLCD

IPv4 IPv6 Ethernet

☐ Obtain IPv4 address automatically

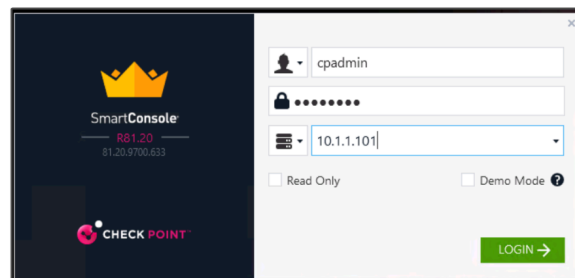
☒ Use the following IPv4 address:

IPv4 address: 20 . 0 . 0 . 1

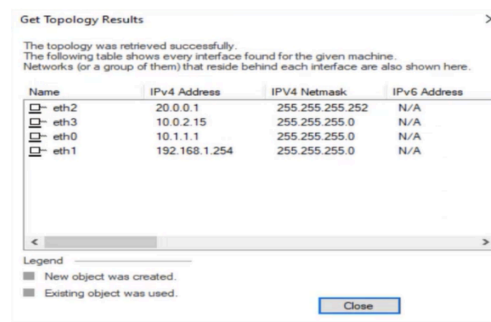
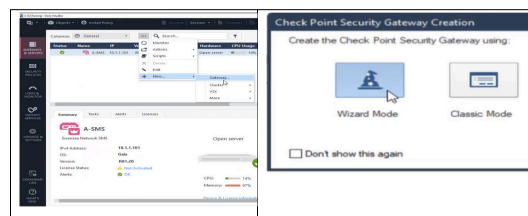
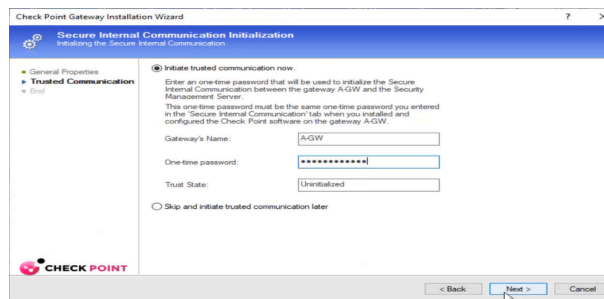
Subnet mask: 255 . 255 . 255 . 252

OK Cancel

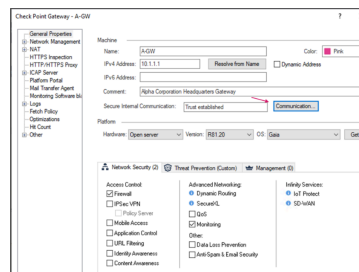
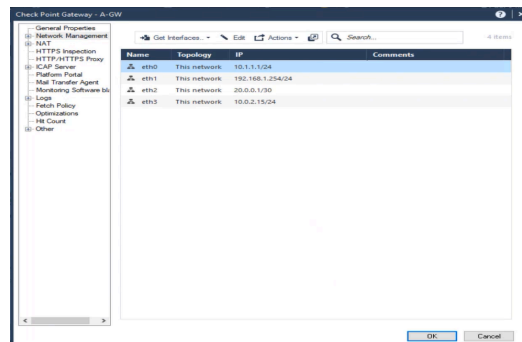
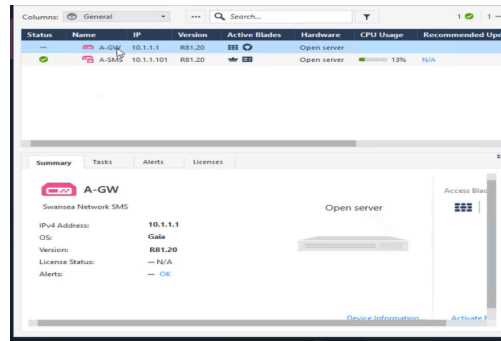
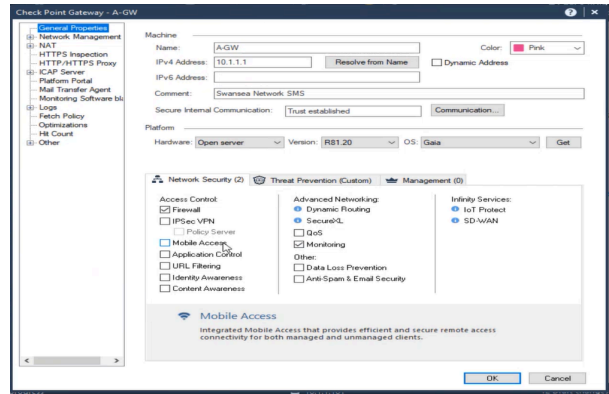
Establishing Secure Internal Communication



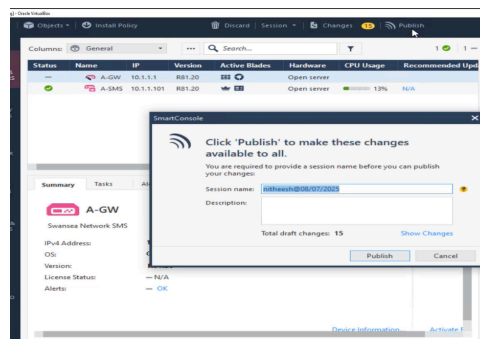
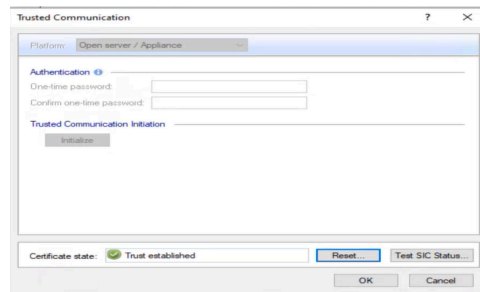
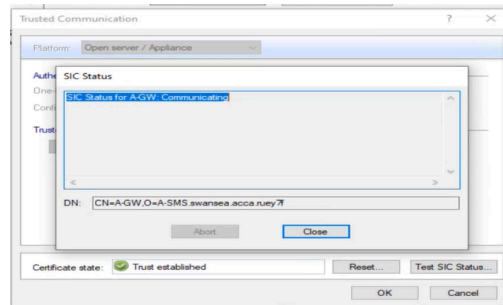
The administrator initiates the gateway integration by logging in to the SmartConsole management client using the username cpadmin in a management server address 10.1.1.101. Inside the console, a new gateway object is created using the step by step Wizard Mode. The key task is to establish a Secure Internal Communication (SIC). This is done by entering the same one time password as was pre-configured on the gateway, along with the gateway's name, A-GW. After SIC trust is confirmed, SmartConsole automatically pulls down the full network layout of the gateway, displaying each interface (and its assigned IP address) for review.



After the gateway object has been created, the administrator enables the Mobile Access software blade in its properties. This triggers the remote access VPN connection capability of the gateway. The interface configuration contained in SmartConsole is then updated so it shows the full list i.e. eth0, eth1, eth2 and eth3 and their respective IP addresses to confirm. The integrated A-GW object is now visible in the main management dashboard, which has an integrated summary panel showing the successful addition of the object. A final review of the properties of the gateway is done to ensure that the name and IP address are correct, and most importantly, that the Secure Internal Communication (SIC) state is "Trust established" to complete the process of adding the gateway to the managed environment.

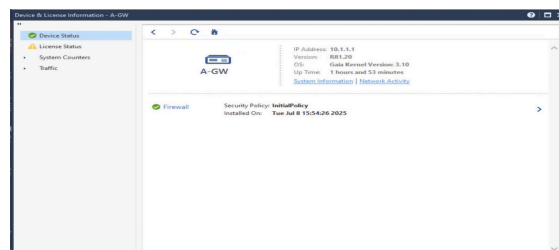
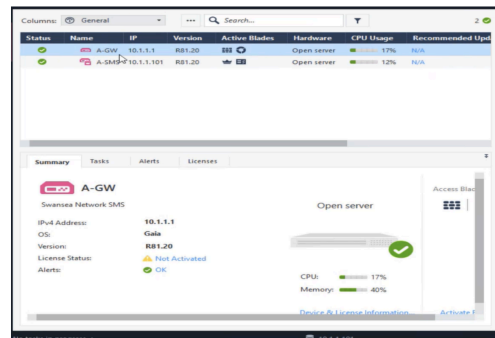
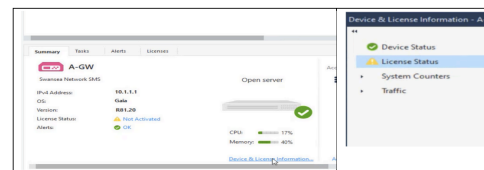
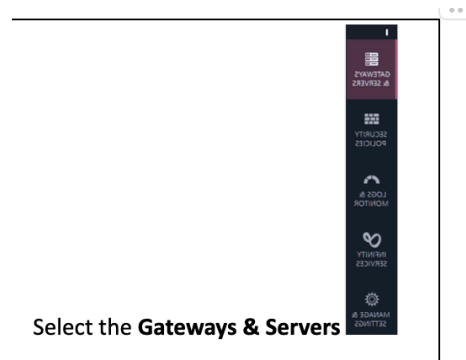


The screenshots show the final phase of the Security Gateway configuration in SmartConsole, including focusing on the check of the Secure Internal Communication (SIC) trust. The administrator tests the connection by going to the window called "Trusted Communication", where that connection is established, with a "Trusted" status, indicated by a green check marks. Another test is done by clicking on "Test SIC Status" which returns the message "SIC Status for A-GW: Communicating." This ensures legitimate and active communication connection between management server and gateway. The process is complete after closing the verification dialogs and clicking "Publish" on the toolbar - the new gateway and its settings are saved to the management server's database.



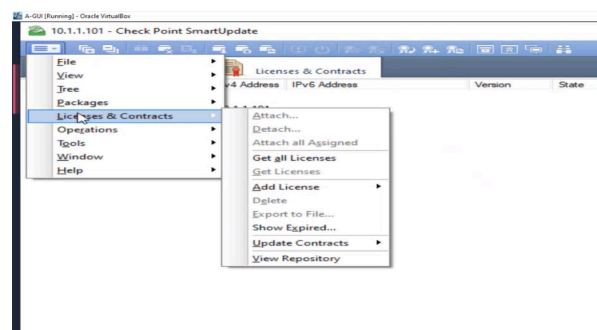
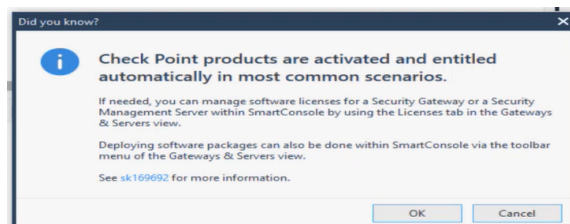
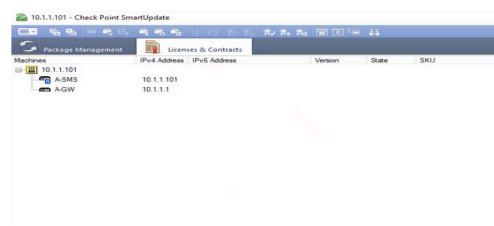
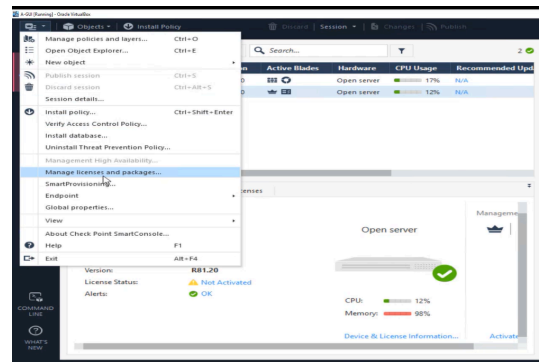
Managing Licence

The visual documentation describes the terminal verification and commit operation for the configuration of the Security Gateway within the SmartConsole management client, with regard to the Secure Internal Communication (SIC) state. Administrative verification is done through the "Trusted Communication" interface with the operational status confirmed by an affirmative mark of a green icon. A second diagnostic procedure is started by executing the "Test SIC Status" command and one receives an output from the system which confirms the successful communication: "SIC Status for A-GW: Communicating." This output is used to verify the integrity and operation of this encrypted control channel between the management server and the gateway appliance. The closing of verification interfaces and activation of the "Publish" function from the SmartConsole command toolbar complete an administrative session.

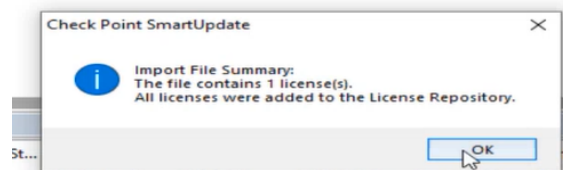
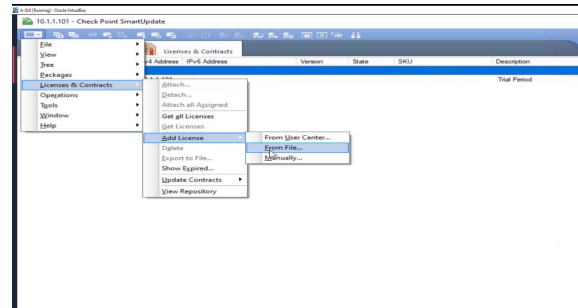


Attaching a Licence Using SmartUpdate

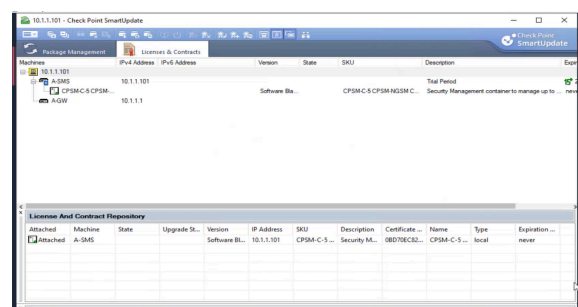
The license administration procedure is started by authenticating to the SmartConsole management client and issuing the application menu navigation call to the "Manage licenses and packages" utility. Following the recognition of a system notification regarding the description of Check Point's automated activation framework, the SmartUpdate management console is displayed, which offers a topological view of all enrolled devices, including the A-SMS management server and the A-GW security gateway, for example.



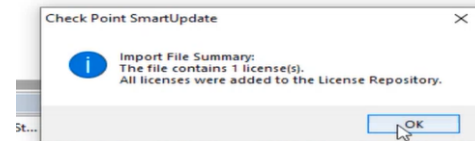
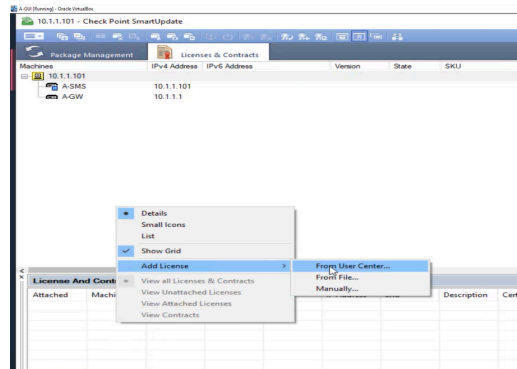
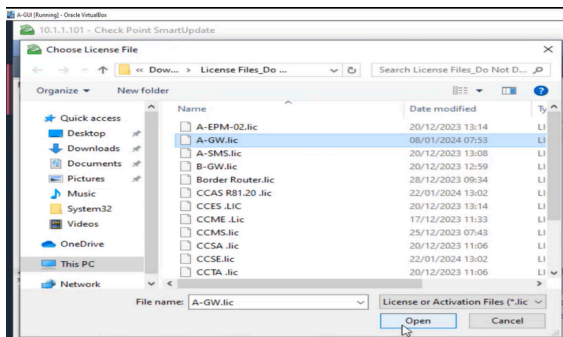
The administrator goes to the "Licenses & Contracts" menu option and invokes the "View Repository" command, which opens up the centralized License and Contract Repository interface. To import a new license, the administrator goes to the repository pane and does a right click to select "Add License > From File" and then select "From File". operation. This initiates the browsers of the local file system, which makes the upload of the necessary license file easier. A confirmation dialog is created if successful parsing and ingestion of the license data into the repository has been done. The administrator completes the operation by choosing "OK" to dismiss the confirmation, which completes the import process and establishes the license for allocation of a managed asset.



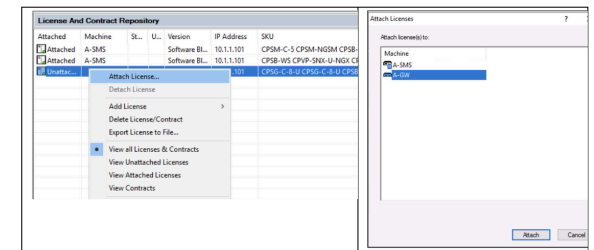
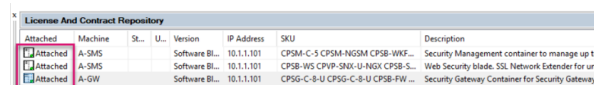
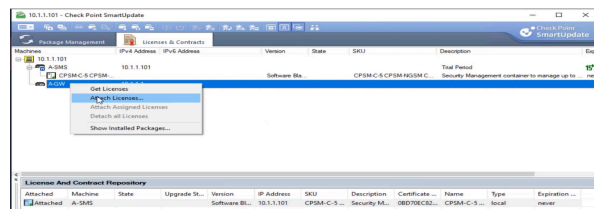
The licensing procedure is completed in the Check Point SmartUpdate management console. The administrator initiates the process of importing files by right-clicking on the License & Contract Repository pane and clicking the "Add License > From File" command. Through the next file system browser the desired license file (e.g. A-GW.lic) is identified and loaded, which opens a system confirmation dialogue about the successful addition of license to the repository. The operation is completed by the administrative verification in the main interface of SmartUpdate: the repository pane should now show the just added license entry completed with a status of "Attached." This



verifies the license is properly linked with respective devices (e.g. the A-SMS) and active, with a permanent validity being indicated with the expiration field typically having a value of "never".



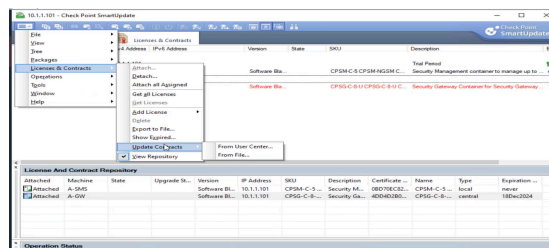
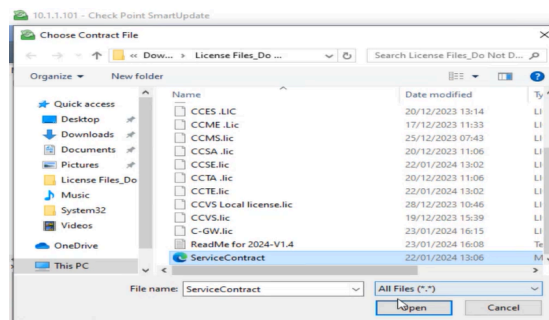
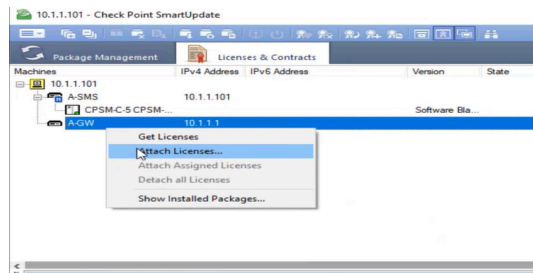
License administration involved within the Check Point environment is centralized from the SmartUpdate console from the "Licenses & Contracts" tab. This interface gives a hierarchical topology of managed network objects like the Security Management Server (A-SMS) and the Security Gateway (A-GW). Entitlement assignment may be performed using two approaches: select a device object, and call the "Attach Licenses" context-menu action, or choosing an unassigned license from the License And Contract Repository pane and deploying it to a target appliance by way of the attachment dialog. Completion of workflow is indicated by a change in status in the repository; licenses indicate the state "Attached," which means the entitlements of the software to access to both the



management server and the gateway appliance are correct and active.

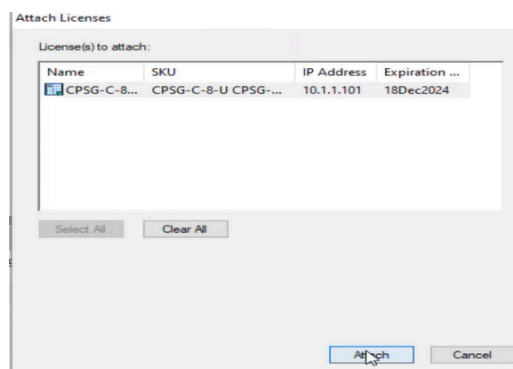
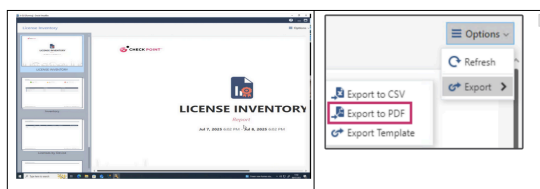
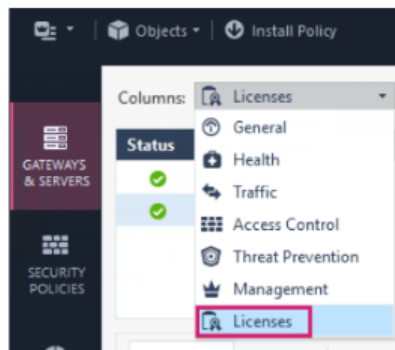
Update the Service Contracts.

The documentation provided describes the main workflow of administering software licenses and support contracts in the Check Point SmartUpdate console. Initially the administrator goes to the "Licenses & Contracts" tab to view the managed object hierarchy. The target enforcement point, the A-GW gateway is selected and the "Attach Licenses" contextual command is used to start license assignment. Subsequently, contract updates are done by choosing the "Licenses & Contracts" menu then the "Update Contracts" action. The administrator is then prompted to choose a source of the update: either the online Check Point User Center or a local file system. When the local file option is selected, a "Choose Contract File" dialog is called. The administrator navigates to the relevant directory, clicks on the designated contract file (e.g. "ServiceContract"), and clicks on the "Open" command to import the contract data into the SmartUpdate repository.



Generating a Licence Report

Administrative license management in the SmartConsole environment means to change the view of the "Gateways & Servers" dashboard. The activation of the "Licenses" column uncovers relevant fields in the state of the license, namely "CK" and "SKU" - and so identifies unlicensed assets, such as the A-GW security gateway. To do a full audit, the "License Inventory" reporting function is run from the "Actions" menu, with the result being exported in PDF format for archival purposes. The process of remediation of the unlicensed state is accomplished by passing through the license attachment workflow, which ends with the "Attach Licenses" dialog interface. Within this dialog, the needed license is chosen and deployed to the target device by pressing the "Attach" command button.



Firewall Rules Configuration and Policy Implementation

Firewall Rules Configuration and Enterprise Security Policy Implementation

The screenshot displays the Check Point SmartConsole interface for configuring firewall rules. The main workspace shows a table of rules with the following data:

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	sdm ftp to gui	A-GUI	SDC	Any	ftp	Accept	Log	Policy Ta...
3	Cleanup rule	Any	Any	Any	Any	Drop	None	Policy Ta...

Below the rules table, the 'Logs' tab is selected, showing a list of log entries. The table includes columns for Time, Origin, Source, Source User, Destination, Service, Access Rule N., Policy, and Description. The log entries show traffic from A-GUI to A-GW for echo-request (SCMP) services, with actions ranging from 'Dropped' to 'Accepted'.

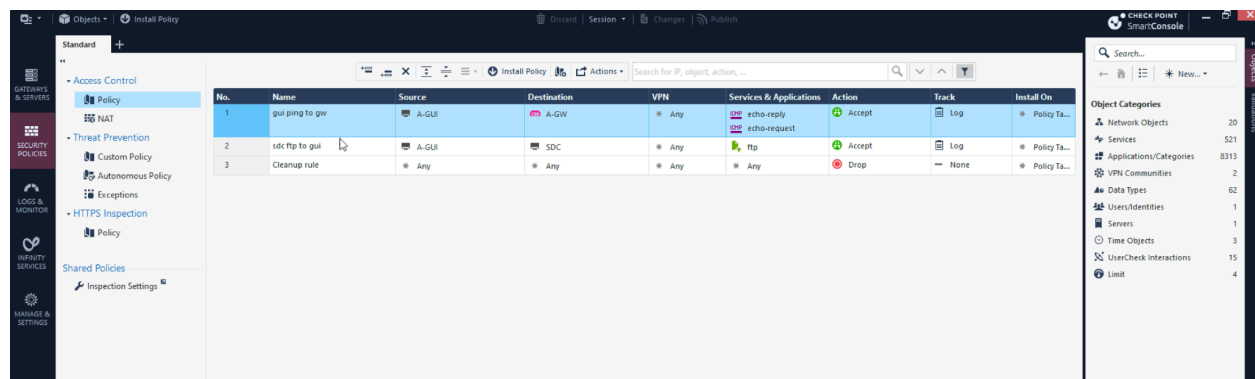
The interface also features a left-hand navigation bar with sections like 'Access Control', 'Threat Prevention', 'Custom Policy', 'Autonomous Policy', 'Exceptions', 'HTTPS Inspection', and 'Shared Policies'. On the right, the 'Object Categories' panel lists various categories such as Network Objects, Services, Applications/Categories, VPN Communities, Data Types, Users/Identities, Servers, Time Objects, UserCheck Interactions, and Limit.

The screenshot below shows the Check Point SmartConsole - the centralized graphical administration interface for Check Point security deployments. This console unifies policy management, object configuration and monitoring functions through a unified dashboard, which increases efficiency in operations. The layout of the interface has a navigation bar on the left side, which gives access to main modules such as Gateways & Servers, Security Policies, and Logs & Monitor. Opposite, in the Object Categories panel can be found the searchable repository of security objects, network services and application definitions to support the construction of modular policy rulebases.

The central working space is taken by the Security Policy editor with the Access Control layer visible. The policy consists of an ordered sequence of rules, in which the rules are handled in the order of the list. The example configuration includes special permissive rules for the services of ICMP (echo-request) and FTP followed by a last overarching Cleanup with Drop action. This type of structure implements a "positive security model" - any traffic that does not match an

explicit allow rule is denied. Rule attributes define source and destination objects, specific services, an action (Accept or Drop) as well as track logging status.

Policy configuration within SmartConsole uses a drag-and-drop methodology which is aimed at reducing configuration errors. New rules are defined by using the New Rule function and the fields are filled by dragging relevant entities from the Object Categories library. Subsequent to policy edits, the administrator has to run the command Install Policy from the toolbar. This process is the compilation of the rulebase and distributing it to the managed enforcement gateways, which activates the policy on production traffic



ICMP Configuration

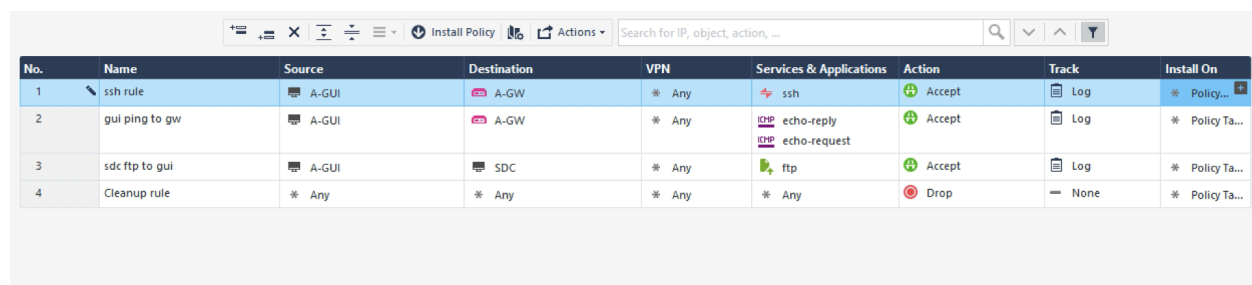
The ping diagnostic utility is a tool that is universally deployed in the network because it leverages the Internet Control Message Protocol (ICMP) for the verification of host reaches and the measurement of the round-trip latency of a packet. ICMP operates at the network layer and it is separate from protocols which handle the transport of data packets like TCP or UDP and is reserved for error signaling and operational query mechanisms. It means that a standard ping operation includes the sending of an ICMP Type 8 (echo-request) packet to a target host to which an ICMP Type 0 (echo-reply) should be sent to receive a reply. These message exchanges provide very important network status intelligence such as measurements of latency and packet loss that make them invaluable for basic connectivity analysis and fault isolation in IP-based networks.

The authorization of traffic through ICMP requires strategic consideration of operational requirements versus posturing of security. While a well-done block of ICMP echo requests (a "stealth" setting) can obscure the network topology from passive recon it is simultaneously removing a critical diagnostic option and could hinder normal network operations such as the Path MTU Discovery. Prevailing enterprise security paradigms therefore call for a granular and policy-based approach. This model allows ICMP traffic in the restricted condition - only from the authorized management segments to the designated infrastructure nodes - and a deny-by-default approach from the untrusted zones. This methodology maintains needed

administrative visibility without using a vector for network enumeration and ICMP-based denial-of-service attack.

Operationalization of this selective permission is done within the Check Point framework through definitive rulebase configuration. Exemplified by an access control rule called "gui ping to gw", this procedure will require the explicit identification of the authorized communication end-points: the Source object ("A-GUI") and the Destination object ("A-GW"). In strict observance of the least privilege principle, the "Services & Applications" parameter is assigned to the discrete "echo-request" and "echo-reply" service definitions, and not some permissive protocol range. The Action of the rule is set to "Accept" and the Track attribute is set to "Log." This logging mandate is of the utmost importance, which allows us to have an unedited registry of each ICMP transaction and thus the compliance of our audits and the incidence of anomalous activity within the authorized traffic that reaches us.

FTP Configuration



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

The File Transfer Protocol (FTP) is a standardized application layer protocol providing file transfer that is part of a TCP/IP network that uses a client-server model. Its operation is characterized by the establishment of two independent TCP-connections: a control connection (with the default port 21) for exchange of commands and responses and a separate data connection (historically this is port 20 used in active mode) for transmission of the file contents. This is the architecture that supports authenticated login and file system operations on a remote host on the network, and for that reason, it is a prevalent solution in legacy and internal enterprise data workflows.

A critical security limitation of conventional FTP is the lack of encryption on both the control and data channels resulting in authenticated data and file data being transmitted in plain text soldiers. This vulnerability opens the sessions up to eavesdropping and manipulation attacks. Security best practices therefore require the disallowing of the use of standard FTP in favor of cryptographically secure methods like SFTP or FTPS. In exceptional cases where the continuity of business requires the use of FTP then a policy of strict containment needs to be implemented. This containment is achieved by being very specific about the permissible FTP traffic to authenticated internal hosts only from well-defined communication paths, substantially reducing the protocol's inherent attack surface.

Execution of this containment policy in the Check Point security management framework requires precise rulebase configuration. A representative rule (which is called "sdc ftp to gui") is defined by listing the allowed Source network object ("A-GUI") and Destination object ("SDC"). The protocol definition is indicated by the addition of the "ftp" service which allows stateful inspection of the control connection and dynamic handling of associated data sessions. The parameter "Action" of the rule is set to "Accept," and the "Track" parameter is set to "Log." The resultant session logs are invaluable in security auditing, evidentiary data in the verification of compliance, and in detecting anomalous data transfer activity.

SSH Access Rule

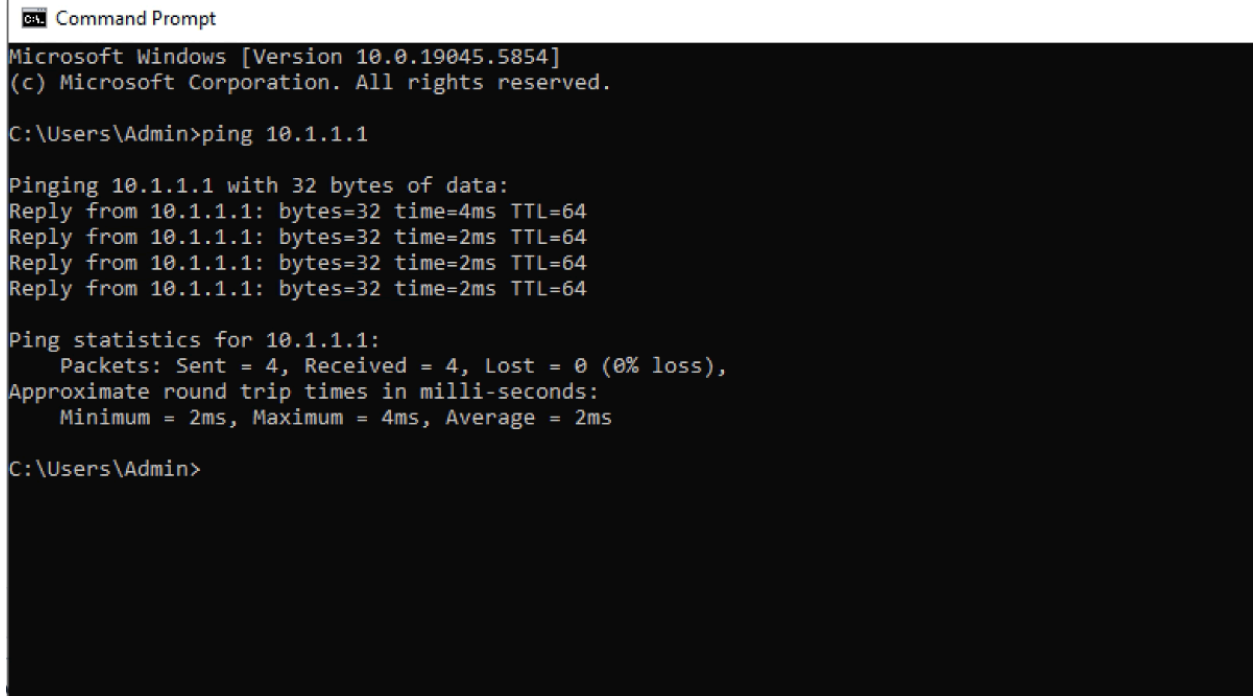
No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	ssh rule	A-GUI	A-GW	* Any	ssh	Accept	Log	* Policy...
2	gui ping to gw	A-GUI	A-GW	* Any	echo-reply echo-request	Accept	Log	* Policy Ta...
3	sdc ftp to gui	A-GUI	SDC	* Any	ftp	Accept	Log	* Policy Ta...
4	Cleanup rule	* Any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

Secure Shell (SSH) is a cryptographic network protocol that is used at the application layer and is designed to provide authenticated and encrypted remote command line interface access. It replaces non-encrypted legacy protocols by using the key exchange algorithms and the symmetric encryption to secure the entire communication session over TCP port 22 and so protect the management traffic from eavesdropping and tampering.

Accessing a computer via SSH is a conferral of higher privilege levels, and therefore requires a strongly controlled security policy. Standard security frameworks recommend narrowing down the two SSH sessions to clearly approved origin addresses (normally committed management workstations) and set out focus on devices. This method of segmentation and restriction minimizes the attack vector within the network, limits the possibility of lateral movement and forces that the network provides comprehensive session logging for audit compliance and security incident investigation.

This control is implemented in the policy rulebase in a Rule 1, named 'ssh rule.' The rule provides the SSH service traffic for a path of communication defined as Source object ("A-GUI") to Destination object ("A-GW"). Having ordinal position in the tip of the rulebase guarantees precedence for administrative traffic. The rule parameters are configured as follows: Action: Accept and Track: Log which allows the connection and creates the required audit trail of all privileged access events which is in accordance with the requirements of security governance.

Validating the policy



```
C:\> Command Prompt
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
Reply from 10.1.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 4ms, Average = 2ms

C:\Users\Admin>
```

The observed successful ICMP echo request/reply transaction adds the empirical validation for the correct implementation of network configuration and corresponding security policy rules. The diagnostic output shows that there is bidirectional IP connectivity between the administrative host "A-GUI" (identified with the IP address 10.1.1.201) and the security gateway "A-GW" at its management interface (with IP address 10.1.1.1). Metrics of 0% packet loss and a round-trip time of ~2ms would be an indicator of an optimal operational state. This connectivity is the direct result of this Access Control Rule 2 ("gui ping to gw"), which has an explicit permit statement on it regarding ICMP traffic between these endpoints.

Making reference to the logical network topology makes it clear on the path end to end. The source host is A-GUI which is in the management network (10.1.1.0/24, designated IntCP). The next-hop router or gateway appliance, A-GW, is the default next-hop for this segment providing a routed route to other security zones that are defined, altogether with the internal corporate LAN (IntSWA: 192.168.1.0/24) and the remote branch network (IntLCD: 192.168.2.0/24), the latter accessible via the inter-site link 20.0.0.0/30. As a result, the successful ping operation is a primary verification operation. It verifies the proper operation of the basic network layer routing mechanism and the proof of proper enforcement of the configured firewall policy, which provides the baseline for a validated administered system before the commissioning of the higher-layer administrative services like Secure Shell or File Transfer Protocol sessions.

```
C:\Users\Admin>ssh admin@10.1.1.1
The authenticity of host '10.1.1.1 (10.1.1.1)' can't be established.
ED25519 key fingerprint is SHA256:PsmPYVGLScDnu5MxDsYnBVBkGdJu0uH10Iys0fVxU4A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.1.1.1' (ED25519) to the list of known hosts.
This system is for authorized use only.
admin@10.1.1.1's password:
```

The following presented screenshot confirms successful initialization of a secure shell (SSH) session from the administrative client to the security gateway at the IP address 10.1.1.1. This operation validates the functional enforce of the dedicated "ssh rule" in the access control policy: this rule allows the transit of TCP traffic to destination port 22. Execution of the `ssh admin@10.1.1.1` command puts the user within the framework of the Trust On First Use (TOFU) security model which requires the user to add explicit acceptance of the previously unknown ED25519 host key fingerprint presented by the gateway. User consent, given through entering "yes," leads to the permanent being placed in the client's `known_hosts` database of the gateway's host key. Subsequently, the now established encrypted session shows the legal configured notification banner and goes to the phase for authentication by password. This sequence conclusively proves that firewall policy configuration is correct and the application layer connection request is succeeding its way through the security infrastructure and reaching the SSH authentication service on the gateway.

Enhanced Security Implementation Through Advanced Features

Application Control and URL Filtering are defining functionalities in the scope of the Next Generation Firewall (NGFW) generating capabilities to inspect granularly and apply policy at the application layer. These capabilities are important when it comes to countering modern-day threat vectors that use permitted network services and web platforms to perform malicious operations. Their implementation has a direct impact on organizational risks that can be attributed to the unauthorized use of applications (shadow IT), non-productive internet use, violations of regulatory obligations due to uncontrolled data transfers, and exposure to web-based threats.

The implementation of these features is defined by an administrative workflow. To do so, valid feature licensing requirements, the Application Control and URL Filtering Software Blades must be started on the target security gateway objects through the SmartConsole management interface. Subsequently, the Access Control Policy layer has to be modified to process data from applications and URLs; this is done by editing the access control policy layer properties and activating the "Applications and URL Filtering" property.

Policy formulation is concerned with the formulation of discrete rules to meet discrete security and administrative goals. A primary security rule is set up that forbids risk categories of applications. This rule is defined with a Source of "Any" (internal networks), a Destination of "Internet" and the Services & Applications field filled in with relevant categories such as "Anonymizer" and "P2P File Sharing". The Action is set to "Drop" and the UserCheck option is enabled to provide user notification of the policy violation.

For operational management, additional rules based on the advantages of Identity Awareness can be built. These rules define an Access Role (e.g. "GeneralStaff") as the Source, "Internet" as the Destination and include application categories such as "Social Networking" in the Services & Applications category. The Action is again set to "Drop"; a configured UserCheck message to communicate the policy basis allowing acceptable use policies to be transparently enforced.

Temporal policy enforcement strengthens security postures by limiting access to resources within a set time frame, limiting the value of the network attack surface, and allows access to align with operational needs. This control covers such use cases as limitation of non-essential access to business hours, enforcement of maintenance windows, compliance with temporal separation-of-duties mandates and management of bandwidth utilization.

Time Objects are created in the management database and implementation begins. These objects define enforcement window(s), which include attributes for time of the day, day(s) of the week and date(s) to which it applies. Under Access Control rulebase, the Time column needs to be enabled to allow time-based assignments.

A standard implementation is a rule pair for internet access for users. The first rule, which authorizes traffic (such as the services of the http, https, etc.) from a given user group ("GeneralStaff") to a given destination ("Internet"), with the Time field filled by the corresponding "Business_Hours" Time Object, and the Action is "Accept". A rule directly following these parameters is to imitate these parameters but without the time restriction and set the Action to "Drop." This is a logical construct that guarantees access is explicitly allowed within the defined temporal boundary and otherwise denied and recorded for security monitoring purposes.