

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

MSc (Cybersecurity and Digital Forensics)

Enterprise Network Security

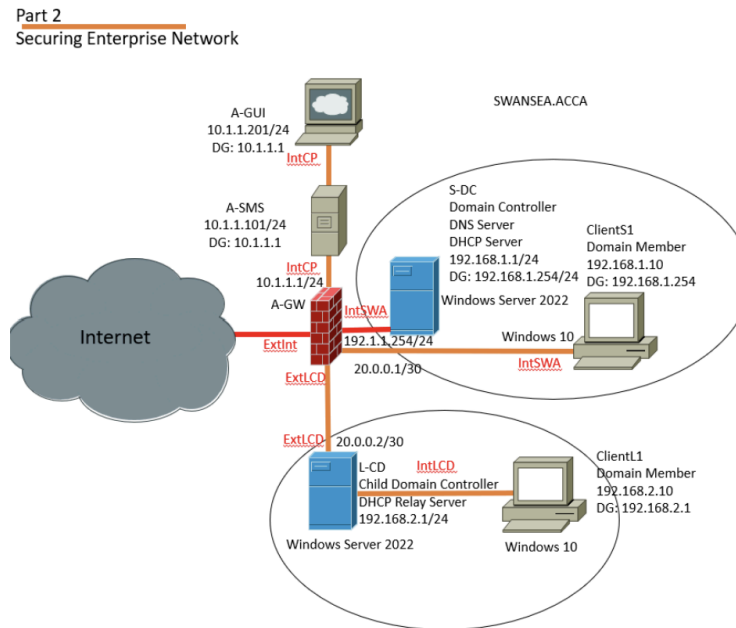
Module code: ACCA7032

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.....	28
Enhanced Security Implementation Through Advanced Features.....	30

Introduction

Overview of the Enterprise Network



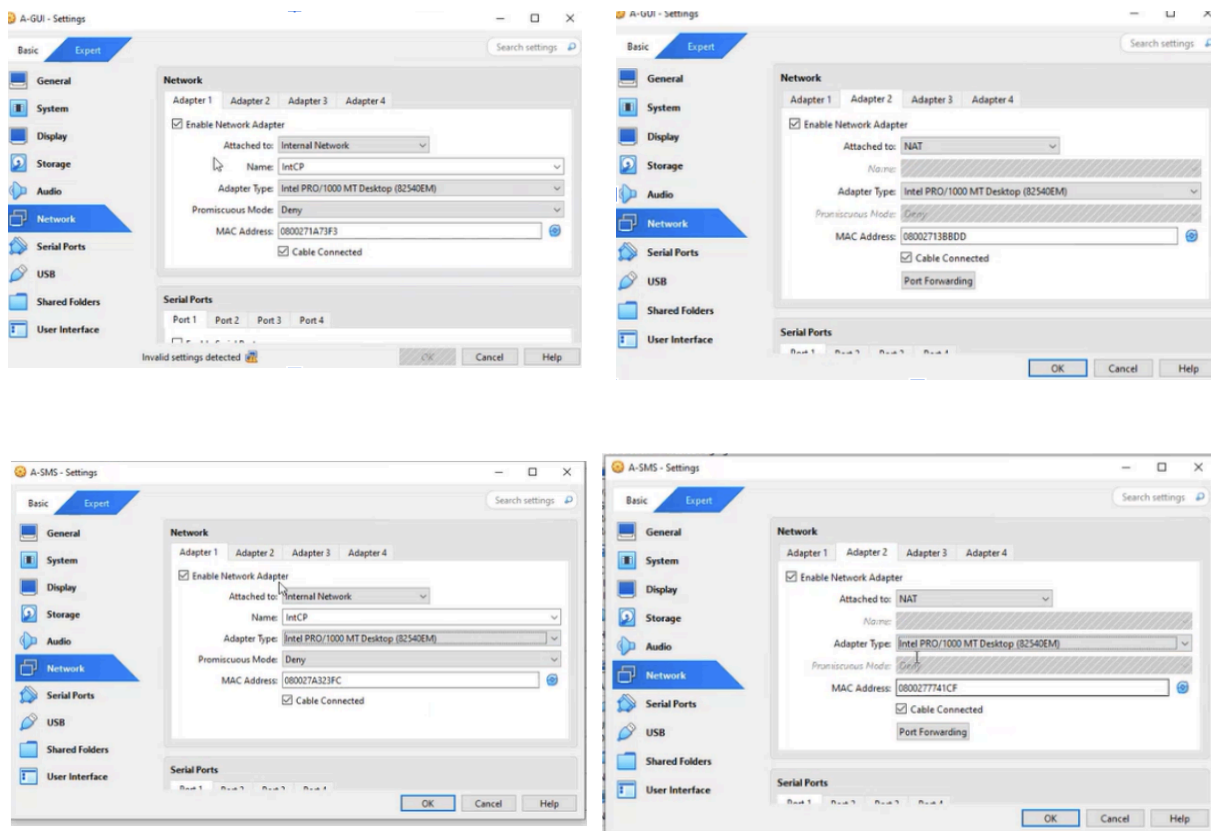
The enterprise network being considered is a hybrid architectural paradigm: the traditional Windows-based service infrastructure is being combined with a dedicated Check Point security enforcement layer. As shown in the topology provided, the environment is divided into two main organisational locations; SWANSEA.ACCA and LONDON.SWANSEA.ACCA. These sites are connected together via a dedicated point-to-point routed link using the 20.0.0.0/30 subnet creating a wide area network (WAN) backbone that allows communication and resource sharing between sites.

The SWANSEA.ACCA site is the network core and main administrative site. It has the root Active Directory Domain Controller (S - DC) configured with the IP address 192.168.1.1/24. This server plays several important roles such as Domain Name System (DNS) resolution, Dynamic Host Configuration Protocol (DHCP) service provisioning and centralised identity and policy management via Active Directory Domain Services (AD DS). One client workstation in this subnet is deployed, called ClientS1 (192.168.1.10), which belongs to this domain. On the other hand, the LONDON.SWANSEA.ACCA site is in the form of a child domain with a supplementary domain controller (L-CD, 192.168.2.1/24) that is configured as a DHCP relay agent and a corresponding client (ClientL1, 192.168.2.10).

A major architectural improvement is made by placing a Check Point security suite into a segregated management network segment (10.1.1.0/24). This suite contains three main appliances: Security Management Server (A-SMS, 10.1.1.101), which serves as the main repository for policy and acts as the administrative hub; the Security Gateway (A-GW, 192.1.1.254), which is located as the default gateway (192.168.1.254) for the Swansea LAN to enforce traffic inspection; and the Administrative Graphical User Interface workstation (A-GUI, 10.1.1.201), from which the Smart Console management application is This topology implements a hub-and-spoke security model quite effectively, in which all traffic destined to or originating from the protected internal networks is forced to pass through the security gateway for policy enforcement and threat inspection at its entire.

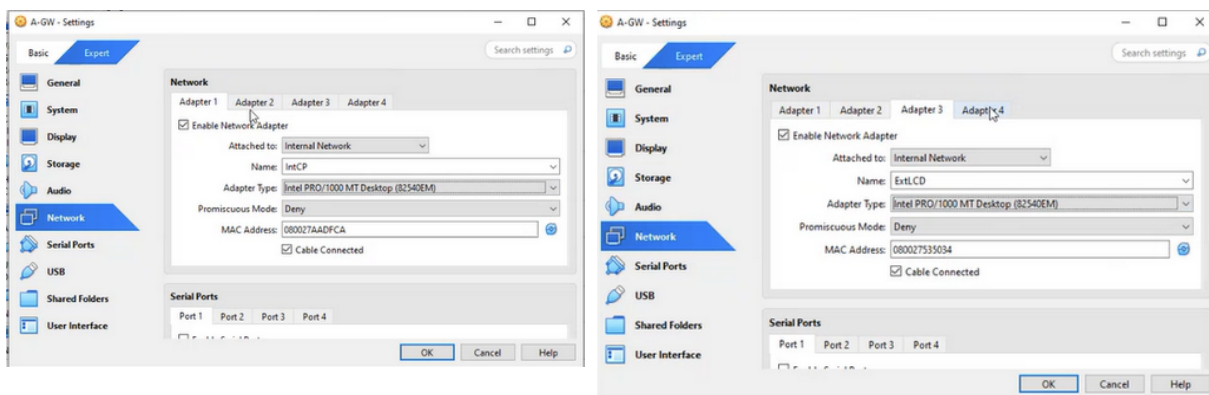
Installation and Configuration of Lab

Configuring Network Settings



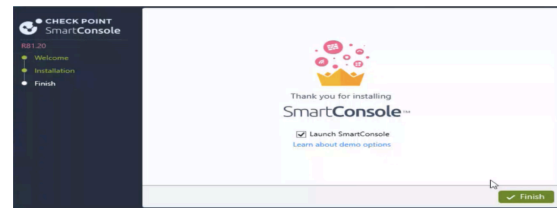
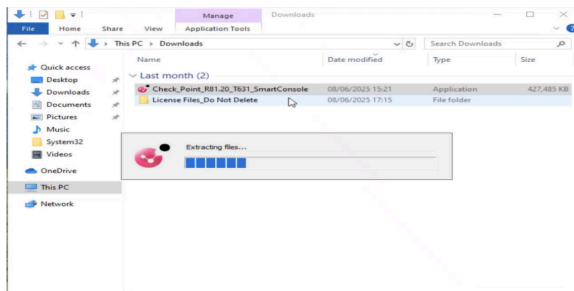
The network infrastructure of the Check Point laboratory environment is built on a strict segmentation strategy which uses virtual network adapters of Oracle VirtualBox. The management plane is isolated to a dedicated internal network switch, designated "IntCP", to connect to Adapter 1 of the management client (A-GUI), Security Management Server

(A-SMS), and Security Gateway (A-GW). The trusted layer ensures that sensitive command and control traffic, policy installation processes and log transmission activities are kept strictly segregated from production user traffic. In order to support the necessary operational maintenance, both the management workstation (A-GUI) and the management server (A-SMS) are provided with secondary adapters in the NAT mode. This design provides the required outbound connectivity on the Internet that is needed for software updates, license checks, threat intelligence retrieval through the use of the physical host, all without compromising the integrity of the segregated internal segments of the laboratory.



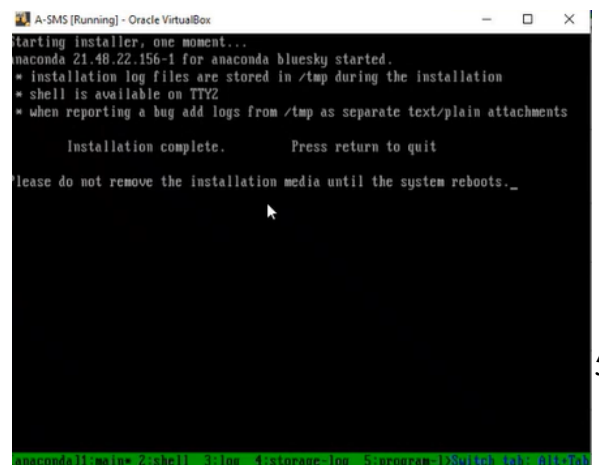
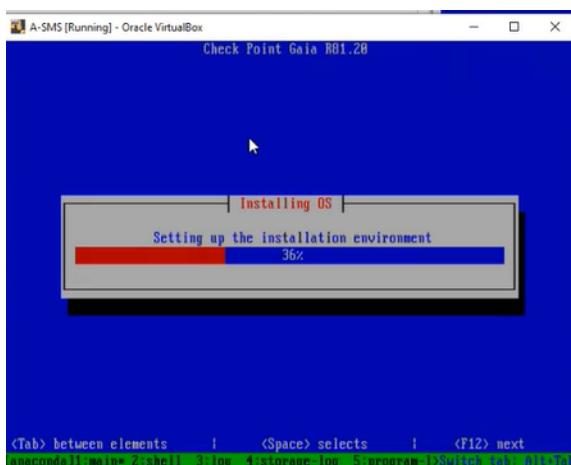
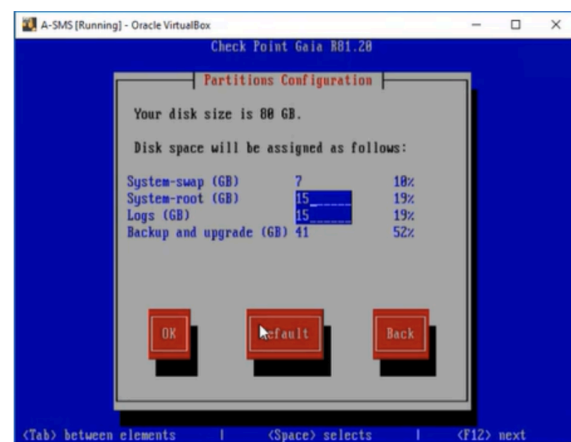
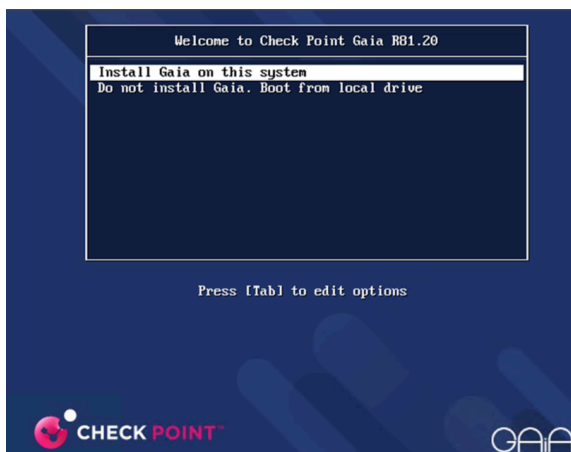
The Security Gateway (A-GW) plays the role of the central enforcement point; it has a multi-interface setup that is a faithful representation of a typical enterprise topology. In addition to its management connection on the "IntCP" network, the gateway has different adapters for managing different flows of traffic: Adapter 2 implements NAT to simulate an external connection to the internet for outbound routing; adapter 3 interfaces with the "IntSwa" internal network, to service the Swansea headquarters LAN (SWANSEA.ACCA); and adapter 4 connects to the "ExtLCD" network, thus modeling a WAN connection to the remote branch in London. The exact definition of responsibilities at four different interfaces allows the gateway to mandate very well-defined security policies to control the relationship between the management zone and the corporate LAN, the corporate LAN and a remote branch office, and the corporate LAN and the untrusted public internet.

Installation of SmartConsole on A-GUI

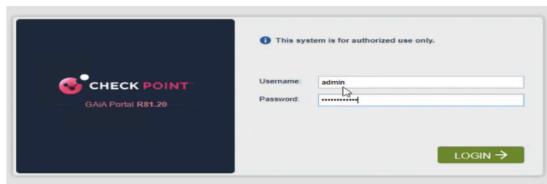


The screenshots show the full installation process for the Check Point SmartConsole client on the A-GUI management workstation, starting with the user running the installation executable from the Downloads folder. A running installation, for example, shows on the user interface an "Extracting files..." progress bar, which later changes to a status screen that says that 15 percent of the installation process has been completed. This status screen incorporates promotional content that focuses on the capability of the platform to facilitate efficient automated operations. The process ends with a confirmation screen with the successful deployment of SmartConsole R81.20 and the administrator is therefore able to continue with centralized security management tasks.

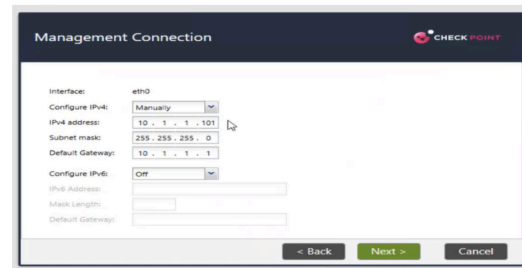
Installing the Primary Security Management Server (A-SMS)



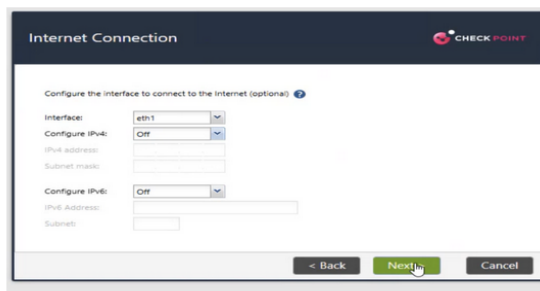
The installation of the Check Point Security Management Server (A - SMS) begins with the booting of the Gaia R81.20 operating system from the installation media. During the initial configuration phase the 80GB storage medium on the target system is divided into separate partitions in line with the standard partitioning schema specified by the installation guidelines. Separate partitions are provided for the root filesystem, system logs, swap space and for later backup or upgrade operations. The automated installation procedure then goes on to copy the necessary operating system files to the newly configured partitions. This phase ends with a confirmation message that the installation was successful, after which the system needs to be rebooted in order to complete the installation and switch to the newly installed Gaia environment.



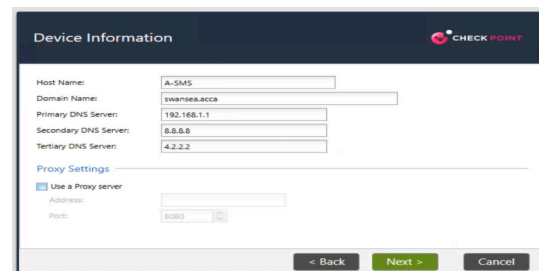
The login screen for the Check Point Gaia Portal R81.20. It features the Check Point logo on the left and a login form on the right. The form includes fields for Username (pre-filled with 'admin') and Password (masked with dots). A 'LOGIN' button with a right arrow is at the bottom right. A note at the top right states: 'This system is for authorized use only.'



The 'Management Connection' configuration screen. It shows settings for the 'eth0' interface. The 'Configure IPv4' dropdown is set to 'Manually'. The IPv4 address is '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, which are currently empty. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom.

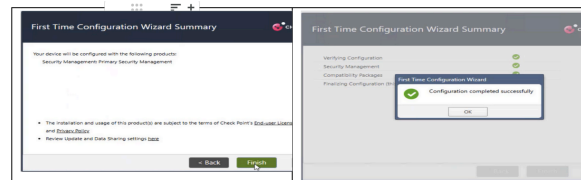
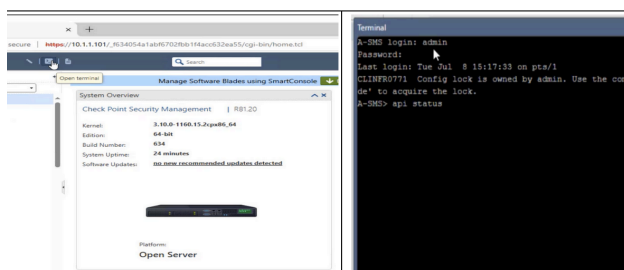
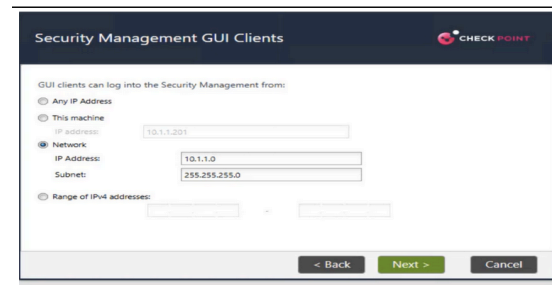
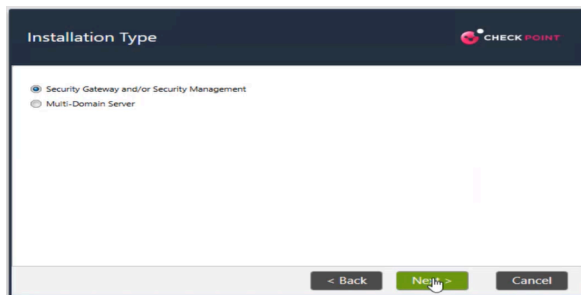


The 'Internet Connection' configuration screen. It prompts the user to 'Configure the interface to connect to the Internet (optional)'. The 'Interface' dropdown is set to 'eth1'. The 'Configure IPv4' dropdown is set to 'OFF'. There are fields for IPv4 address, Subnet mask, IPv6 address, and Subnet, all of which are empty. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom.



The 'Device Information' configuration screen. It contains fields for Host Name ('A-SMS'), Domain Name ('swarses.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 a section for 'Proxy Settings' with a checkbox 'Use a Proxy server' (which is unchecked) and fields for Address and Port (set to '8080'). Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom.

After the system reboot, the administrator logs in to the Gaia Portal through the A-GUI client's web browser and authenticates in order to start the First Time Configuration Wizard. An essential phase of the wizard requires the manual configuration of the principal management interface (eth0), to which the static IP address 10.1.1.101, the subnet mask 255.255.255.0 and the default gateway 10.1.1.1 are assigned, in order to integrate the server with the laboratory's management network on a secure basis. The setup of the secondary, internet facing interface (eth1) is left for a later stage. This first network configuration lays the foundation of the server's core connectivity, including communication within the management plane and placing the server for further stages of the configuration wizard.

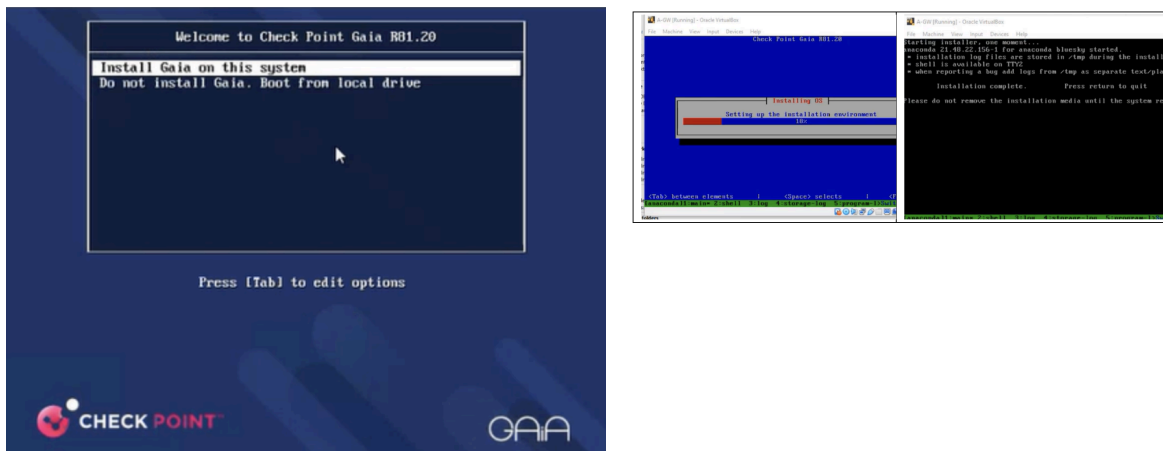


The First Time Configuration Wizard is used to set up key identity and functional roles for the Security Management Server. The device is registered as "A-SMS" and forms part of the "swansea.acca" domain, where the DNS resolution is mostly directed at the internal Domain Controller located at 192.168.1.1, in order to enable local identity awareness, auxiliary external DNS servers are used to support redundancy for internet based updates. The type of installation is clearly specified as "Security Gateway and/or Security Management" because it

is intended for a single-organization laboratory environment, and therefore does not require the complexity of Multi-Domain Server setups designed for service providers.

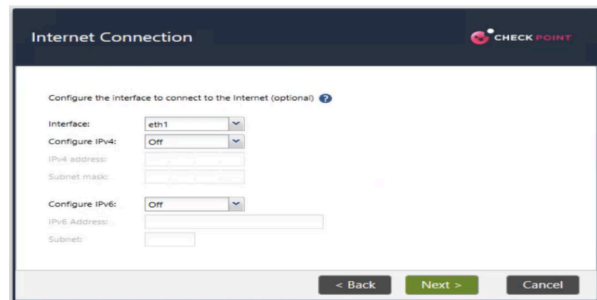
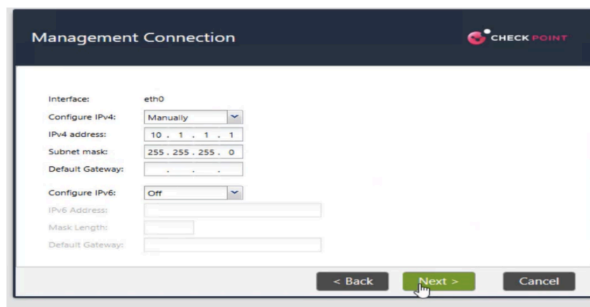
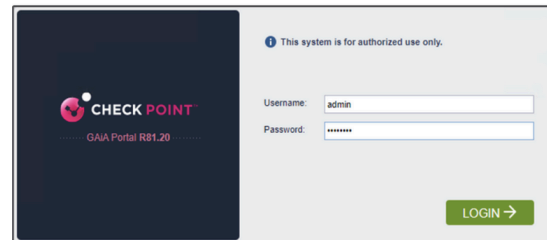
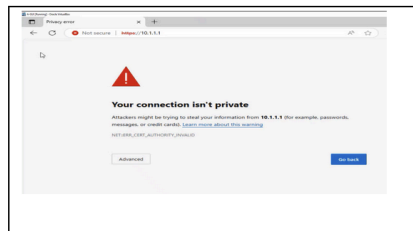
Subsequent to the selection of the product access controls are put in place to limit administrative privileges so that connectivity is only allowed from the designated 10.1.1.0/24 management subnet. This measure ensures that only duly authorized workstations - such as the A-GUI client - get access to the server via SmartConsole. The wizard ends with a summary page stating that the successful deployment of these configurations as a "Primary Security Management" server has been completed. The final verification is noticed through the Gaia Web UI; in this interface the System Overview dashboard shows the operational status of the R81.20 appliance, and a terminal command is shown to be performed to verify the operational state of the API server.

Installation of the Check Point Gateway (A-GW)



The installation of the Security Gateway (A-GW) starts from booting the virtual machine from the Check Point Gaia R81.20 ISO and selecting the Install Gaia on this system option from the startup menu. This action triggers the process of deploying the operating system, which is similar to the process used for the management server. The process is carried out through the automated configuration of the installation environment, which is indicated by a progress bar, and ends with the display of a confirmation message "Installation complete." At this point, the user needs to press Enter to reboot the system and thus complete the initial configuration of the gateway.

Running the First Time Wizard on the Security Gateway



The administrator initially enters the Gaia web portal via the browser on the management client, and to do so they deliberately bypass the standard self signed certificate warning and access the login interface. Upon starting the First Time Configuration Wizard, the network configuration for the primary management interface (eth0) is checked as 10.1.1.1 with a /24 subnet and hence ensuring connectivity with the management server. The configuration of the internet facing interface (eth1) is deferred with both IPv4 and IPv6 disabled at this point. Critical device identity parameters are then developed which sets the hostname "A-GW" and domain "swansea.acca" and DNS hierarchy leading to the internal controller 192.168.1.1 and then to public resolvers for any redundancy purpose.



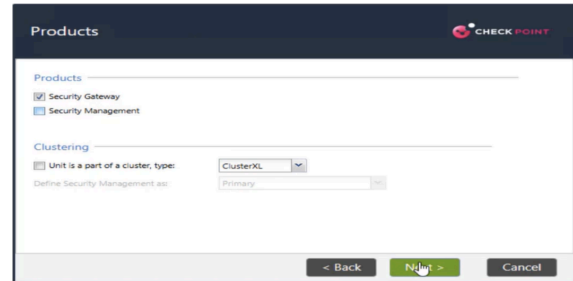
Device Information

Host Name: A-GW
 Domain Name: swansea.acca
 Primary DNS Server: 192.168.1.1
 Secondary DNS Server: 8.8.8.8
 Tertiary DNS Server: 4.2.2.2

Proxy Settings

☒ Use a Proxy server
 Address:
 Port: 8080

< Back Next > Cancel



Products

☒ Security Gateway
☐ Security Management

Clustering

☐ Unit is a part of a cluster, type: ClusterXL
 Define Security Management as: Primary

< Back Next > Cancel

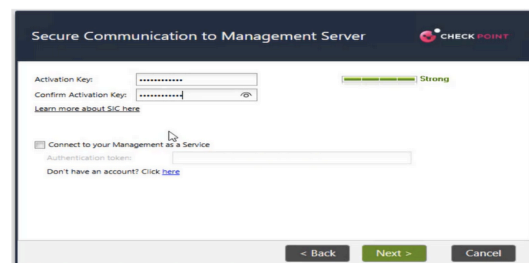


Dynamically Assigned IP

Does this gateway have a dynamically assigned IP address (DAIP gateway)?

☐ Yes
☒ No

< Back Next > Cancel



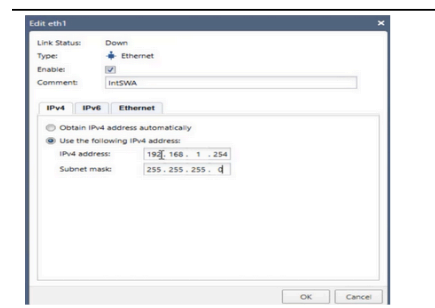
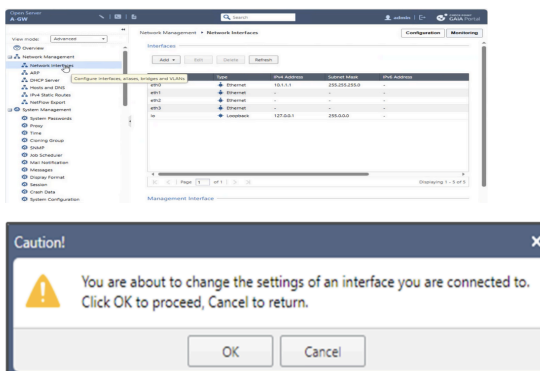
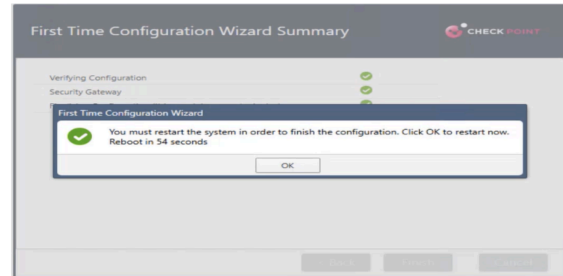
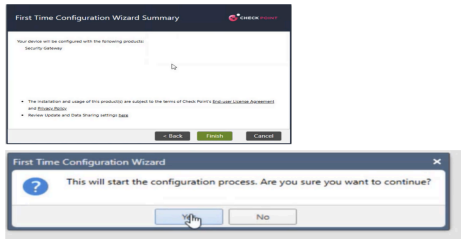
Secure Communication to Management Server

Activation Key: *****
 Confirm Activation Key: *****
[Learn more about SIC here](#)

☒ Connect to your Management as a Service
 Authentication token:
 Don't have an account? Click [here](#)

< Back Next > Cancel

The configuration process starts with the specific inclusion of what the appliance is playing the role of; "Security Gateway" is selected while "Security Management" is not checked, thus bearing testimony to its exclusive role as an enforcement point, not as a management server. Clustering is intentionally disabled and the gateway is set to use a static IP address instead of one that is dynamically assigned. The interaction is culminated in the vital establishment of Secure Internal Communication (SIC) where some activation key ("Chkp!234") is inputted to bring in the requisite trust relationship to allow the Management Server to manage and disseminate policies to this gateway.



The configuration of the Security Gateway (A-GW) ends in a summary in a First Time Configuration Wizard, in which the administrator confirms that the appliance is configured as a single purpose "Security Gateway", after which the administrator clicks on "Finish" to apply the settings. Subsequent to a mandatory system reboot needed to initialize the new configuration that has been applied, the administrator re-enters the Gaia Portal to finish the configuration of the network interfaces. Within the section Network Interfaces, it can be seen that the management interface (eth0) is confirmed to be active with the corresponding IP address 10.1.1.1 while the internal interface (eth1) is manually enabled and has an IP address 192.168.1.254, to which the comment "IntSWA" is added, establishing the link of the gateway to the internal Swansea network segment.

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	-

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

Destination Address	Next Hop	Administrative Distance
---------------------	----------	-------------------------

Link Status: Down
 Type: Ethernet
 Enable: ☒
 Comment: ExtLCD

IPv4 IPv6 Ethernet

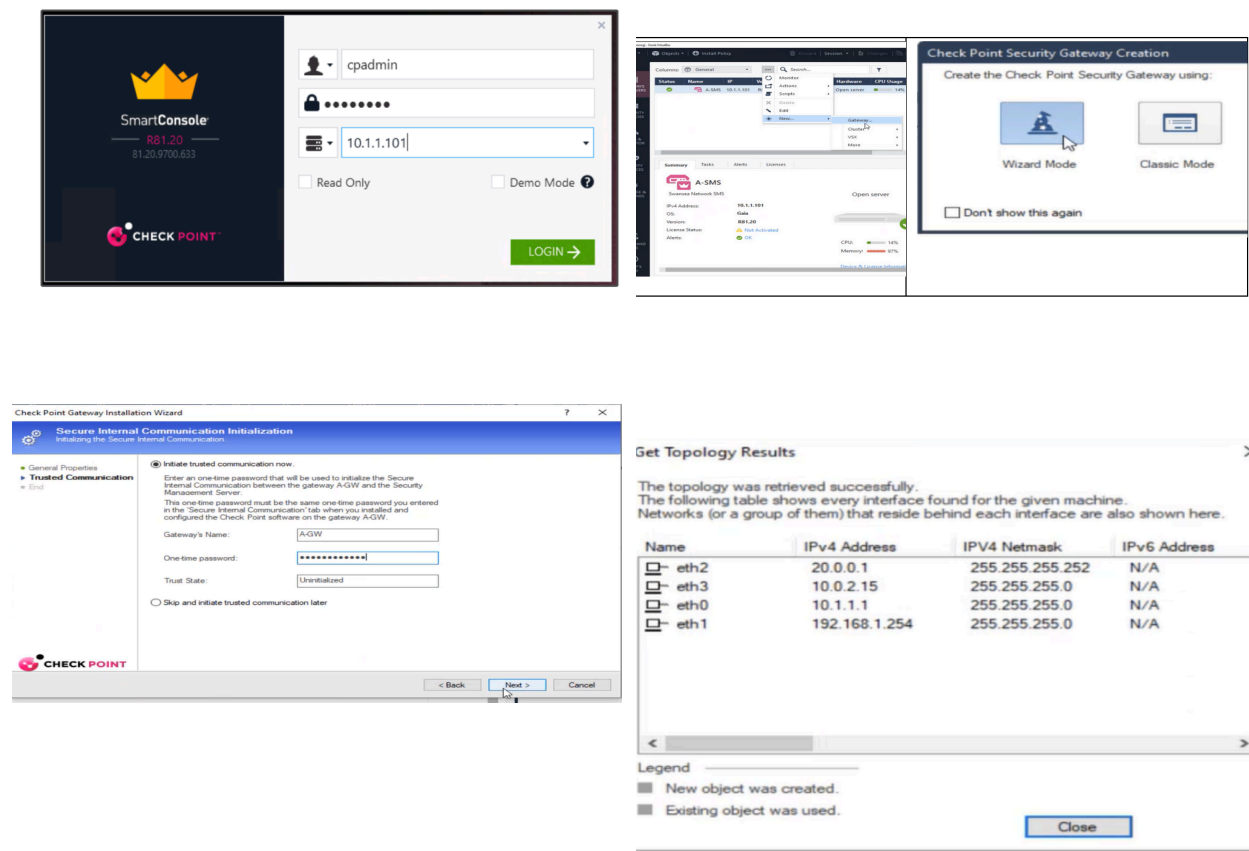
☐ Obtain IPv4 address automatically
☒ Use the following IPv4 address:

IPv4 address: 20.0.0.1
 Subnet mask: 255.255.255.252

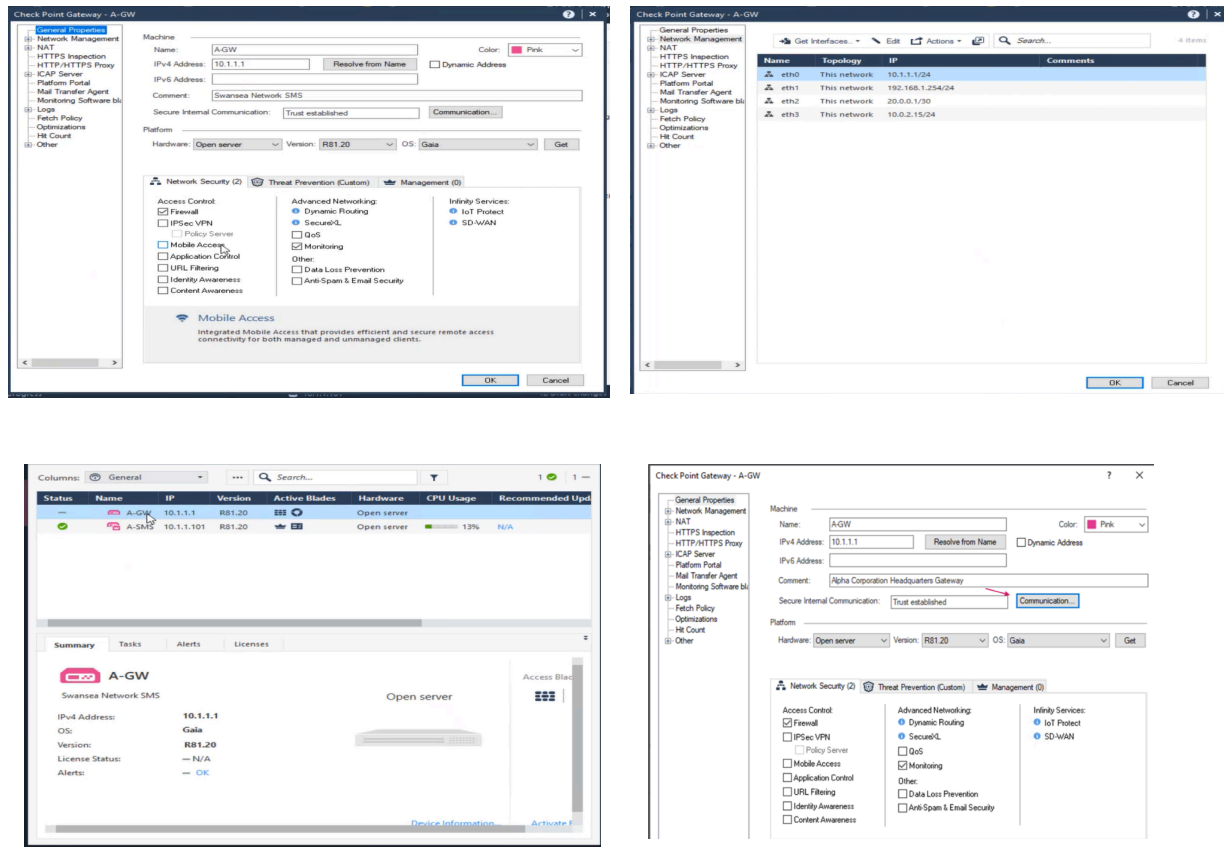
OK Cancel

During this stage of A-GW configuration, the remaining network interfaces are enabled and given their respective roles before the termination of the session. The administrator edits interface eth2 and enables it under the annotation "ExtLCD" and statically assigns it the IPv4 address 20.0.0.1/30 (255.255.255.252) and so sets it up to represent the point-to-point link towards the simulated London Wide-Area Network segment. Subsequently, interface eth3 is selected and configured as an active interface labelled "ExtInt" with the IPv4 parameters set to obtain an address automatically via DHCP and thus will be able to act as a dynamically addressed external or internet-facing interface. Upon application of these modifications, the administrator logs out of the Gaia Portal and kills the browser session, thus formally ending the configuration of the gateway interfaces and ending the laboratory exercise.

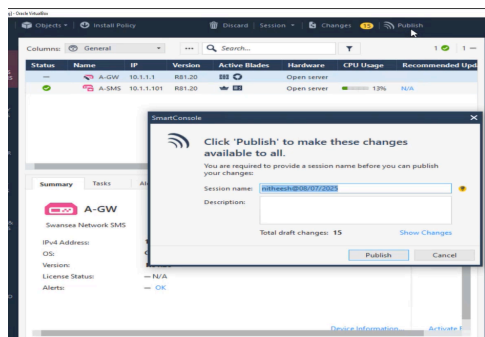
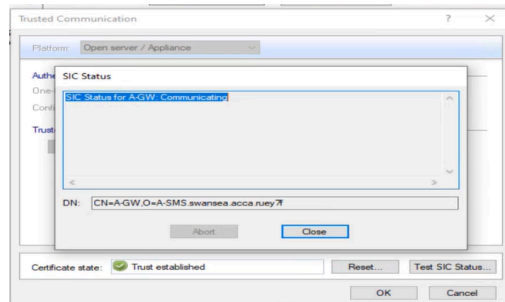
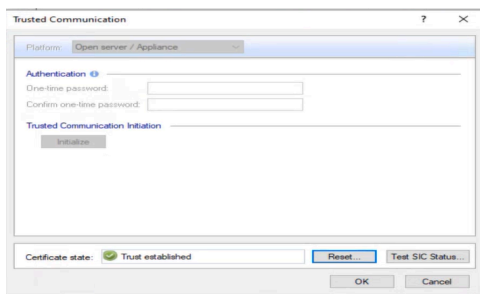
Establishing Secure Internal Communication



To connect the Security Gateway (A-GW) and the management server, the administrator first authenticates to the management server using the SmartConsole client using the cpadmin credentials and the IP address of the server 10.1.1.101. Thereafter, in the console, a new gateway object is created using guided Wizard Mode. The most important part of this procedure is the creation of Secure Internal Communication (SIC); in this part, the administrator creates a trust relationship by providing the identifier for the gateway, A-GW, together with the previously configured one-time password. Upon successful creation of the SIC trust, SmartConsole automatically collects the network topology of the gateway, thus showing all the configured interfaces and IP addresses, to be verified in detail.

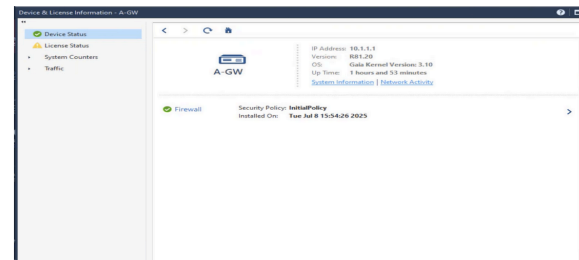
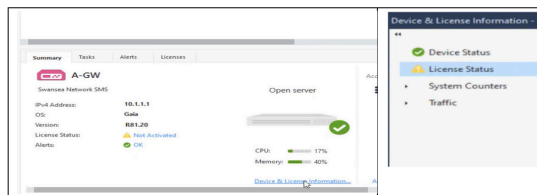
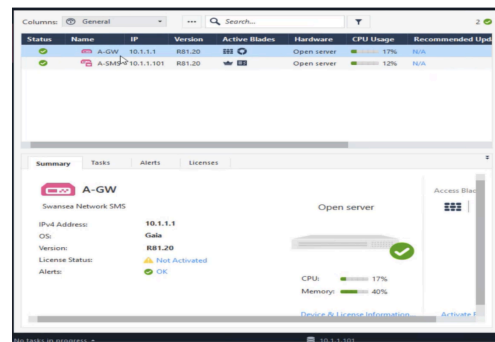
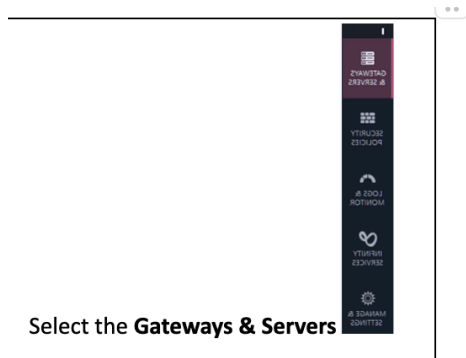


Following the object instantiation, the administrator accesses the Mobile Access component under the properties of the gateway to enable remote access VPN functionalities. The interface list of the gateway including eth0, eth1, eth2 and eth3 with corresponding IP addresses are refreshed and checked in SmartConsole. The newly created A-GW object is then displayed in the main dashboard, where details of the object's summary are available and thus the successful integration is proven. A definitive inspection of the various properties of the gateway assures that the name and IP address are correct and - most importantly - that the Secure Internal Communication status is reported as "Trust established" thus completing the integration of the gateway into the managed security environment.



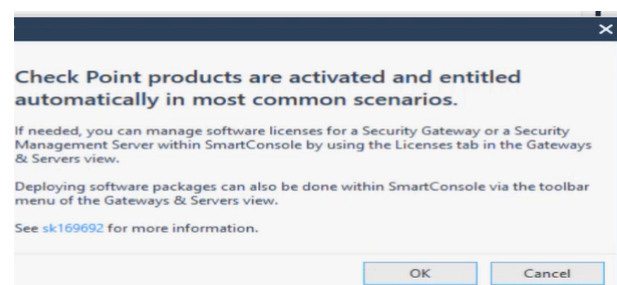
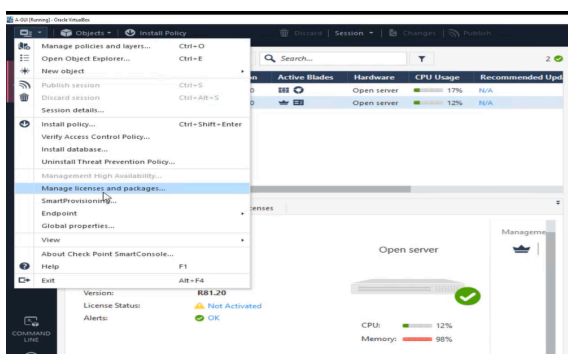
The following screenshots show the final verification and commitment of the configuration on the Security Gateway in SmartConsole, focusing on the trust of Secure Internal Communication (SIC). By accessing the "Trusted Communication" dialog, the administrator will validate the connection, to the point where the status will be "Trust established" with a green checkmark. An additional verification step includes the selection of "Test SIC Status" which returns a confirmation message stating "SIC Status for A-GW: Communicating" thereby verifying that the management server and gateway can exchange information in a secure manner. The procedure ends by closing validation windows and choosing the "Publish" button in the SmartConsole toolbar, so as to persist the new gateway object and changes to its configuration to the management database.

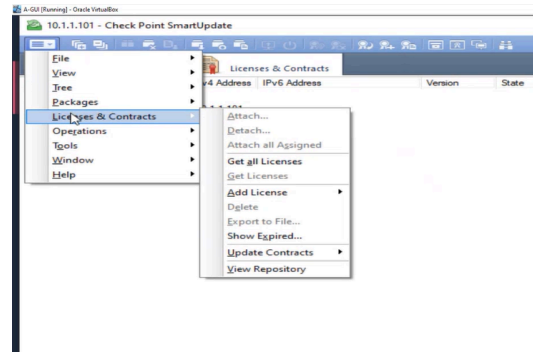
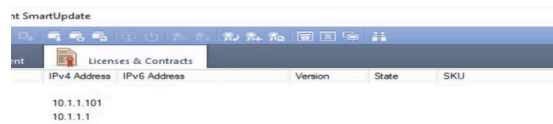
Managing Licence



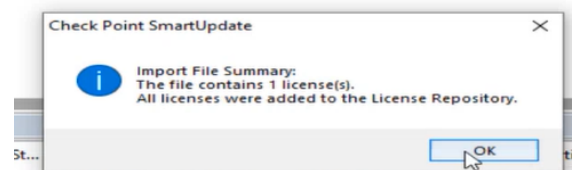
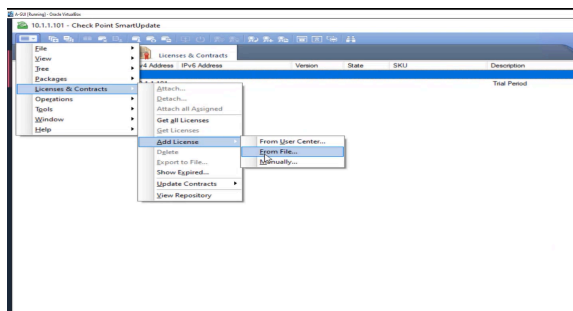
In order to check the licensing status of the newly installed gateway, the administrator opens SmartConsole and goes to the "Gateways & Servers" view. When choosing the A-GW object, an immediate problem is shown in the summary pane in the form of a "Not Activated" status with a yellow warning icon. For a more in-depth analysis, the administrator opens the "Device & License Information" window and selects the "License Status" tab, which presents relevant information such as expiration dates and entitlement validity thus confirming that the gateway requires license activation for it to reach full operational status.

Attaching a Licence Using SmartUpdate

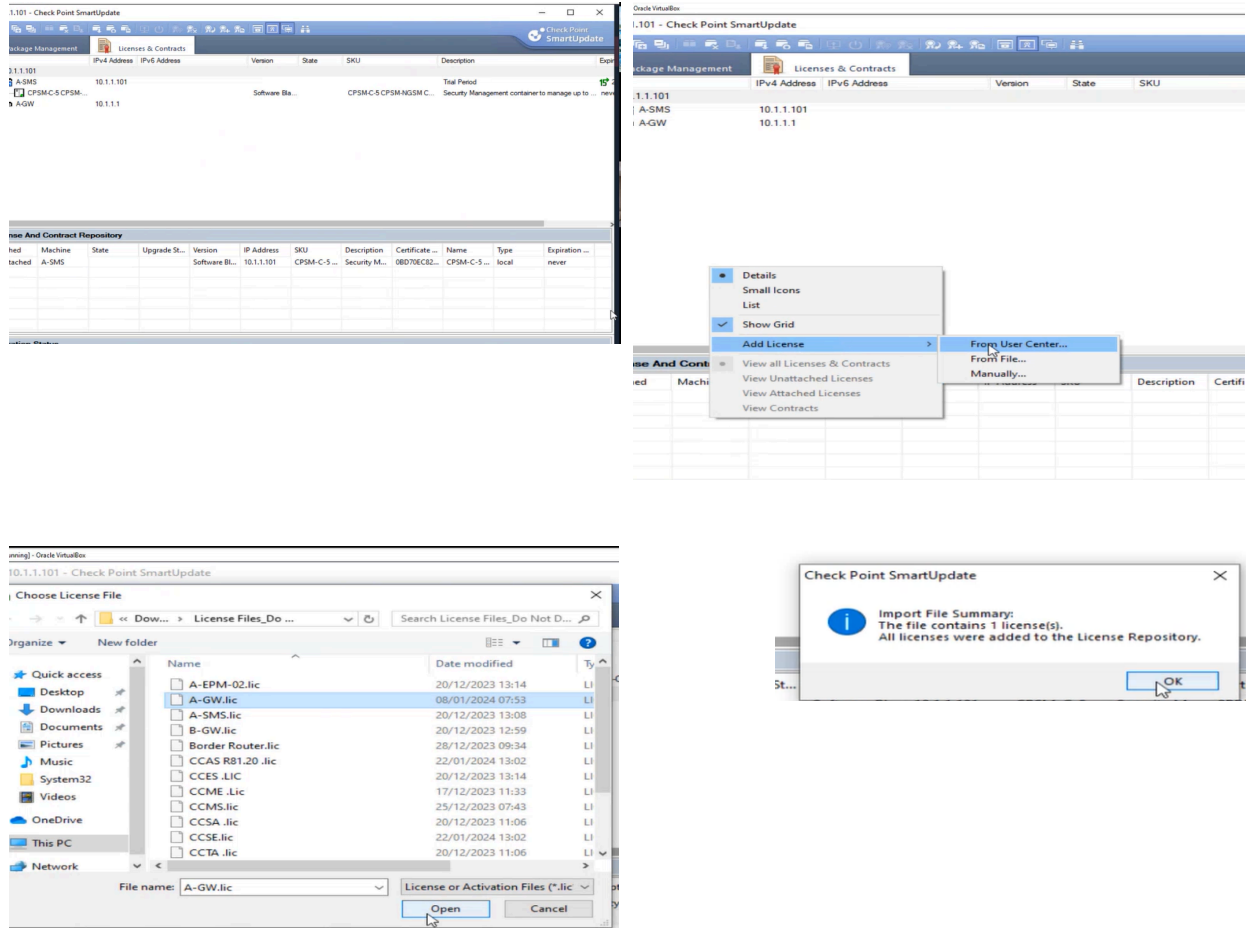




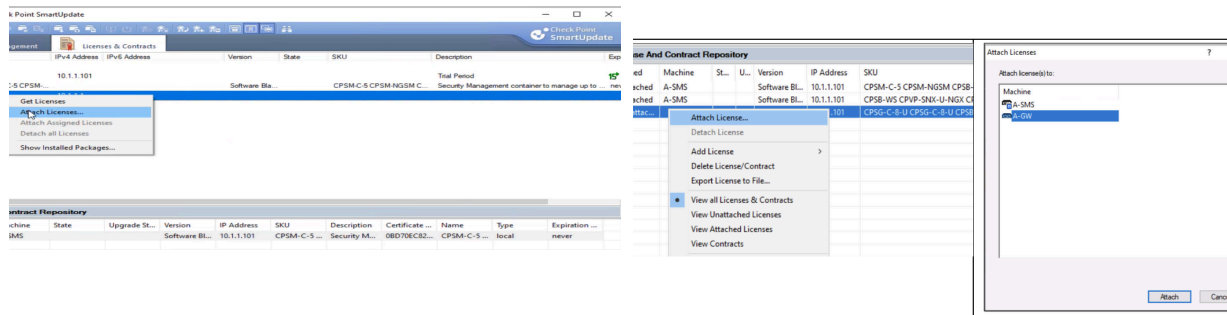
In order to start the license management process the administrator authenticates in SmartConsole and either moves to the principal menu to invoke the "Manage licenses and packages" utility. Subsequent to the contextual informational prompt of a Check Point's automatic activation ability capability the SmartUpdate interface is rendered and provides a hierarchical representation of all devices administered, including the A-SMS management server and the A-GW gateway. From this primary interface, the administrator navigates to the "Licenses & Contracts" menu and clicks on "View Repository", this brings to the central workspace where the unison of all software entitlements is consolidated and managed.



Within the License and Contract Repository, to create a new license the system administrator starts the add process by right-clicking in the pane and then selecting "Add License>From File..." from the context menu. This operation opens a file browser, that allows the administrator to switch to and upload the appropriate license file from the local file system. Upon successful import, a confirmation dialog appears, thus validating that the file contained the necessary license information, and that the file has been imported into the repository. The administrator can reject their confirmation by clicking "OK" which closes the dialog. This action eventually ends the import procedure and makes the new license available for assignment to a managed device.



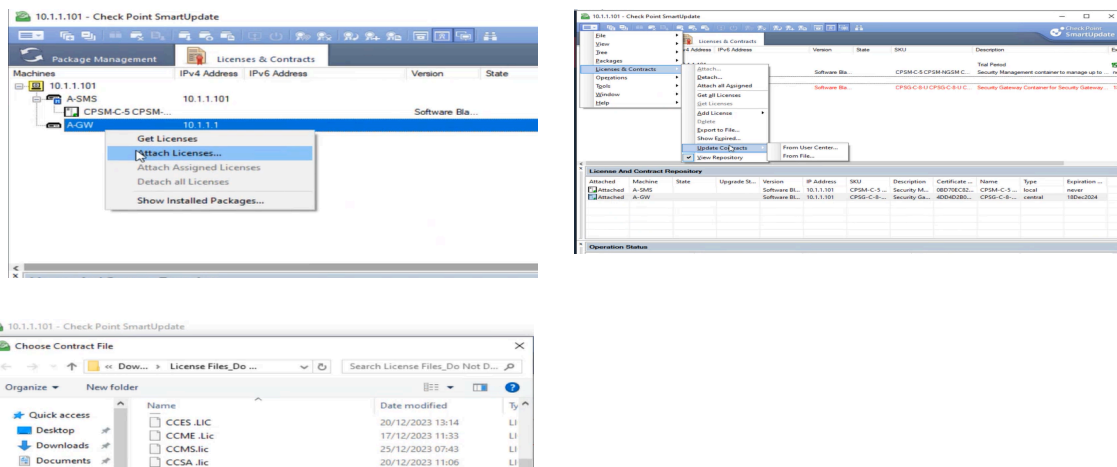
To consummate the licensing procedure in Check Point SmartUpdate, the system administrator inserts the requisite license file by doing a right click within the "License & Contracts" repository pane and clicking "Add License > From File". Within the subsequent file browser, the relevant license file (e.g. A-GW.lic) is found and opened; in this way, an appropriate confirmation dialog is opened to confirm the successful incorporation of the license into the repository. The process is completed with visual confirmation in the principal SmartUpdate window, which should now have the repository pane showing the new entry with an "Attached" status Carnegie, which will also confirm that the license has been accurately associated with the intended device (such as the A-SMS), and that it is active, usually indicated with a "never" expiration date for perpetual licenses).



Repository									
Machine	State	Upgrade St...	Version	IP Address	SKU	Description	Certificate ...	Name	Expiration ...
A-SMS	Attached		10.1.1.101	10.1.1.101	CPSM-C-5 CPSM-NGSM CPSB-WKF...	Security Management container to manage up to...	0BD70ECB2...	CPSM-C-5 ...	never
A-GW	Attached		10.1.1.101	10.1.1.101	CPSB-WS CPVP-SMX-U-NGX CPSB-S...	Web Security blade, SSL Network Extender for un...			
A-GW	Attached		10.1.1.101	10.1.1.101	CPSG-C-8-U CPSG-C-8-U CPSB-FW ...	Security Gateway Container for Security Gateway			

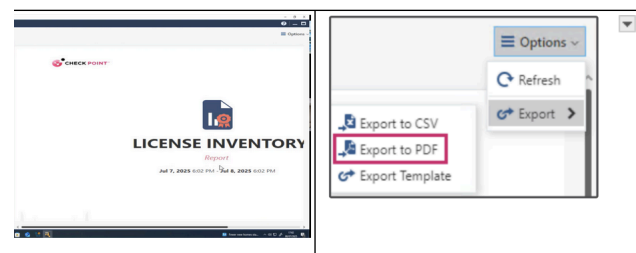
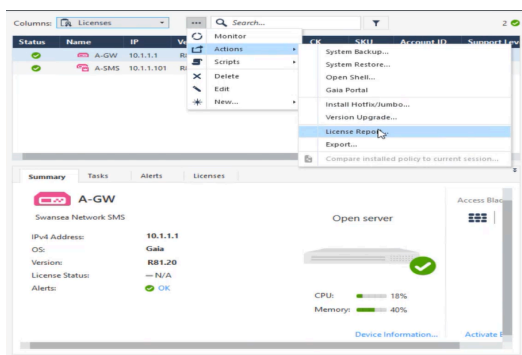
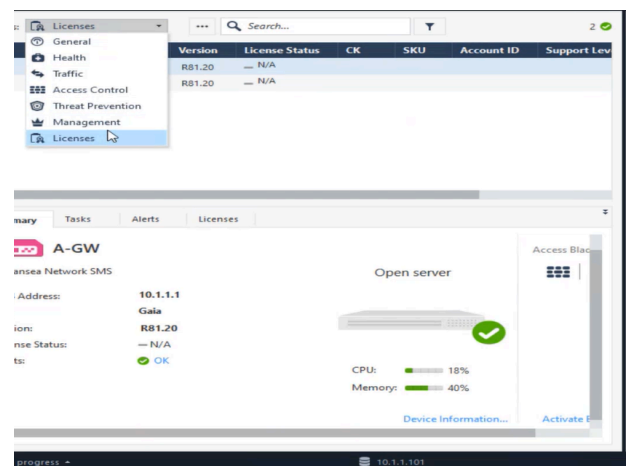
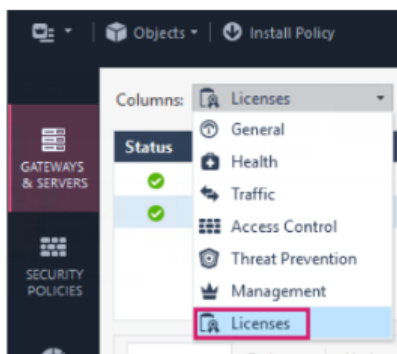
The Check Point SmartUpdate interface supports the centralized control of the licensing through the "Licenses & Contracts" tab, which displays a hierarchical view of network entities such as the Security Management Server (A-SMS) and the Security Gateway (A-GW). Administrators can to assign entitlements they can either choose a specific device (i.e. the A-GW) and invoke the Attach Licenses option in the context menu or pick one of the licenses that are not yet attached to a device from the License And Contract Repository pane and assign it to the desired machine by invoking the Attach Licenses dialog box. Visual confirmation of successful execution of this procedure is present within the repository in the status of the licenses is changed to "Attached" thus indicating that the software entitlements associated respectively with both the management server and gateway are properly bound and actively operational.

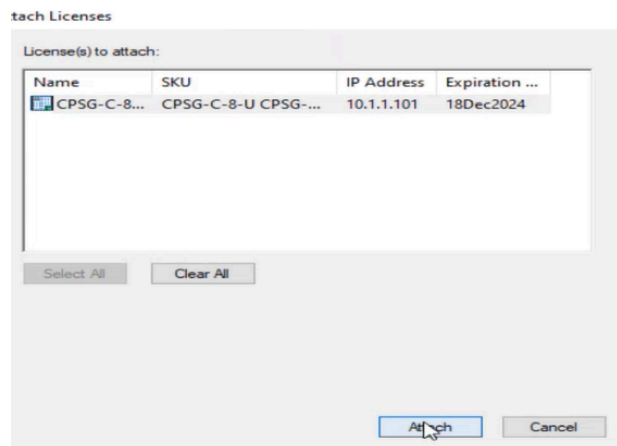
Update the Service Contracts.



The following screenshots outline the major processes of administering licenses and support agreements in Check Point SmartUpdate. First, the administrator uses the "Licenses & Contracts" tab to view the network hierarchy and then selects the A-GW gateway and the "Attach Licenses..." context menu item to trigger the process of assigning a license to the A-GW gateway. Subsequently, in order to update the service contracts, the user navigates to the top menu, selects "Licenses & Contracts" > "Update Contracts" and indicates whether the updates are obtained directly from Check Point's online User Center or from a locally stored file. Finally, when the option of local update is selected, a "Choose Contract File" dialog is used to navigate to the directory holding the license files, to select the proper contract file (e.g., "ServiceContract") and to click on the "Open" button, thus importing the contract into the SmartUpdate repository.

Generating a Licence Report





In order to administer licensing in Check Point SmartConsole, the responsible administrator first customizes the "Gateways & Servers" dashboard by enabling the "Licenses" column. This action reveals specific status indicators, such as "CK" and "SKU," and that A-GW gateway is still unlicensed. For the purposes of exhaustive auditing, the administrator creates a thorough "License Inventory" report via the "Actions" menu before saving the document as a PDF for archival record keeping. Ultimately the administrator corrects the licensing deficiency by going through the attachment workflow, which ends with the "Attach Licenses" dialog: here a particular license is selected and applied to the target device when the "Attach" button is pressed.

Firewall Rules Configuration and Policy Implementation

Firewall Rules Configuration and Enterprise Security Policy Implementation

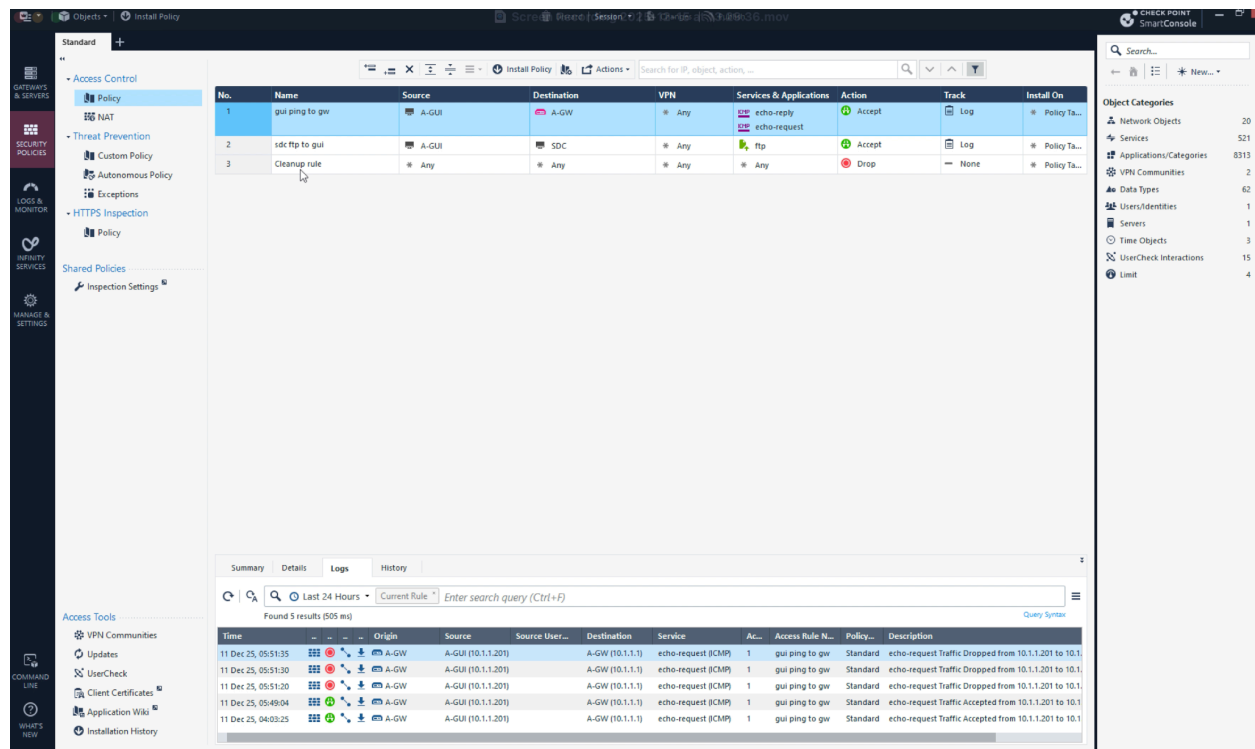
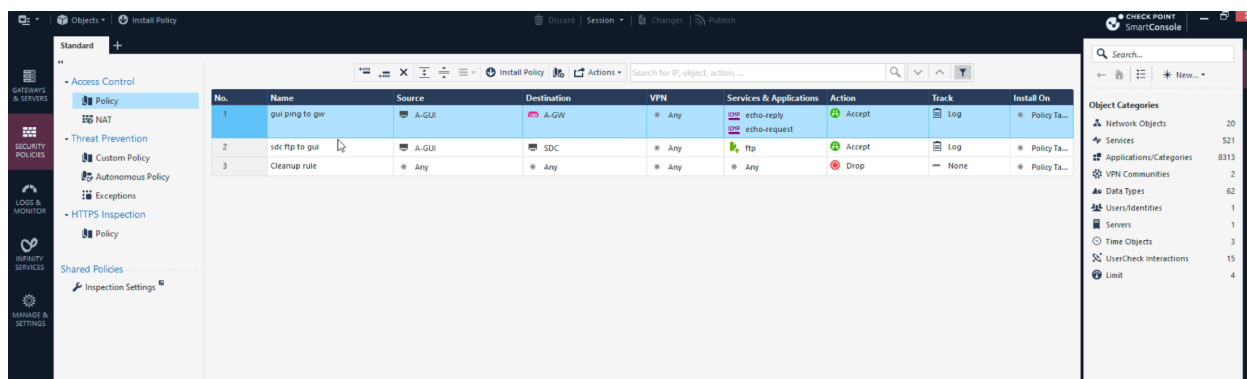


Figure shows Check Point SmartConsole, a consolidated graphical management interface used for managing Check Point security environments. The dashboard fully integrates policy management, object configuration, and real-time monitoring in a unified interface for optimizing the security administrator operational workflow. Within the left hand sidebar, the interface provides easy navigation between the most important functional domains, such as Gateways & Servers, Security Policies, and Logs & Monitor, making transition between rule configuration and traffic pattern investigation easy. The right hand panel ("Object Categories") is a searchable repository of reusable network objects, services, and applications and facilitates the construction of modular and maintainable rulebases.

In the heart of the interface lies the pane of Security Policies especially the "Access Control" layer is where the administrators specify the criteria for passing network traffic. The displayed policy is in the form of an ordered enumeration of rules interpreted one after another from top to bottom; this evaluation determines the status of a given traffic instance with respect to predefined conditions. In the exemplary case illustrated, here, the policy clearly allows ICMP traffic (shown as "gui ping to gw") and FTP file transfers (as shown as "sdm ftp to gui"), followed by a default "Cleanup rule" that drops any traffic not matching any earlier entries, implementing a "positive

security model" where everything that is not explicitly allowed is denied. Each rule is defined by antecedently defined source and destination objects, particular types of services (such as echo-request or ftp) and resultant actions (Accept or Drop) with provisions made for logging, activated to enable an extensive monitoring of policy enforcement.

Configuring the security policy within SmartConsole represents an intuitive draggable and dropable procedural paradigm that is designed intentionally to reduce the incidence of errors. Administrators can create new rules by choosing the "New Rule" icon or by right clicking a rule contextually into this rule base; they then fill out the Source, Destination and Services & Applications columns by transferring objects directly from the right-hand "Object Categories" panel. For example, in order to make changes to an extant FTP rule, the administrator only needs to identify the relevant network object from the auxiliary panel and then drag it into the correct cell so that there is an instantaneous update of the rule definition. Upon completion of modifications, the "Install Policy" button, located in the top toolbar, needs to be activated which will compile and promulgate the modified configuration to the enforcement gateways and assure that the prescribed logic is actively enforced when live network traffic passes through the gateways.



ICMP Configuration

Ping is the most universal utility for network diagnostics, which works through the Internet Control Message Protocol (ICMP) to determine the reachability of nodes, and to measure round-trip delay between nodes. In contrast to transport-layer protocols used for, for example, sending application data, such as TCP or UDP, ICMP is a protocol operating at the network layer, which is mainly used for error notification and operation requests. A traditional ping operation consists of sending an ICMP packet of type IP address echo-request to a target host and waiting for an ICMP packet of type IP address echo-reply to be received. These exchanges provide key feedback information about network status, such as the rate of packet loss and the measurement of latency, and as such, ping is invaluable for initial troubleshooting and connectivity testing of any and every IP-based infrastructure.

The choice to block or not to block ICMP traffic is an archetype of the interdependence between the utility of operations and the security posture. Complete suppression of ping requests, which is commonly known as "stealth mode," can be used to hide internal network topology and hamper basic reconnaissance scans by adversaries. However, this approach simultaneously hinders legitimate diagnostic operations, and it may interfere with Path MTU Discovery and hence resulting in fragmentation complications. Within an enterprise environment, where an organization is already mature, prevailing best practices support the selective permissibility of ICMP. Such a policy allows traffic from authorised management segments, shown in the accompanying screenshot by the "A-GUI" source, to reach certain infrastructure components of designated as "A-GW," and systematically denies traffic of similar types from unauthorised external zones. This nuanced methodology allows administrative visibility to be preserved and exposure to massive ICMP based network mapping and denial of service attacks (ping floods) to be avoided.

In order to implement selective permission in Check Point SmartConsole, an administrator creates a narrowly scoped access rule. As shown in Rule 1 ("gui ping to gw") the configuration starts by identifying the authorized source object ("A-GUI") and corresponding destination object ("A-GW"): That is, it is a rule which is only applicable to this specific transmission path. Within the Services & Applications column the admin authorizes the echo-request and echo-reply service objects or the icmp-proto grouping and not all IP protocols, which is in accord with the least privilege principle. Finally, the action is set to "Accept" to allow the packets, and the track option is set to "Log"; the function of the track option is very important, as it is used to create a record for each ping attempt, which can be used for auditability purposes, that is, to verify the authorized use and to detect any potential anomalies.

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	sdm 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 standard network protocol based on a client and server model which is chiefly used for exchanging files between computing devices on a TCP/IP network. Unlike rudimentary datagram protocols, FTP takes provision for two separate TCP connections: a control channel, which is conventionally run over port 21, for the exchange of

commands and related responses, and a data channel, which again is conventionally run over port 20 or an ephemerally assigned port for the actual transmission of the file content. This dual-channel architecture allows authenticated sessions in which users are allowed to upload, download, and administer files on remote servers which finally make FTP an indispensable medium for data exchange in the unavoidable legacy and intranet-centric enterprise contexts.

While FTP is still operational, the fact that it does not provide encryption poses significant security risks because all data that is sent (in plain text) including user names, passwords, and file contents among others is sent in plain text and vulnerable to packet sniffing and man-in-the-middle attacks. In a secure enterprise environment the default policy should be to disable the standard FTP in favour of secure alternatives such as SFTP (SSH File Transfer Protocol) or FTPS (FTP over SSL). However, when legacy systems or particular internal processes (for example, the "SDC" server interaction shown) require its use, FTP must be highly restricted. Access needs to be limited to designated internal segments, authenticated user access and specific servers to reduce the attack surface, instead of allowing unrestricted FTP connectivity across network perimeter.

Establishing a safe FTP rule in Check Point SmartConsole requires that an administrator strictly define the approved communication channel. Within Rule 3, which is designated "sdc ftp to gui", the administrator specifies the source object "A-GUI", and the destination host "SDC", thus limiting the traffic flow to these two endpoints only. In the Services & Applications column is incorporated the FTP service object whereby the firewall is instructed to interrogate the control channel on TCP port 21 dynamically manage the auxiliary data connection. The Action field is set to "Accept" to authorize the transfer, and, crucially, the Track field is set to "Log" so that all details of the individual file transfer session(s) are maintained, providing an irreplaceable audit trail for the detection of possible data exfiltration or unauthorized access.

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...

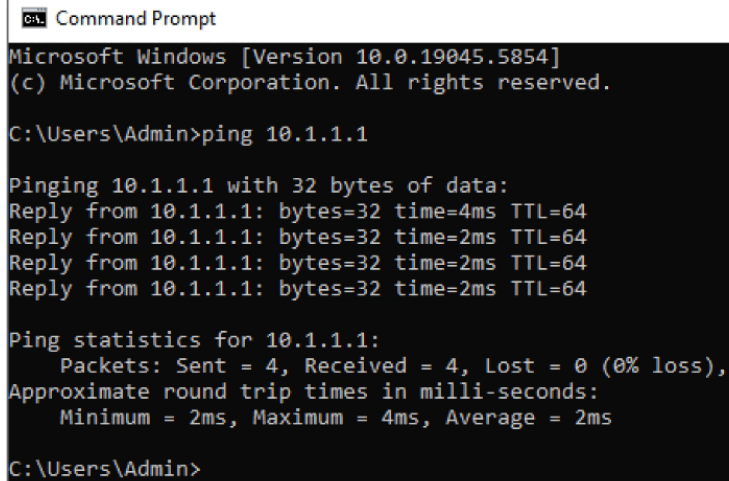
Secure Shell (SSH) is a cryptographic network protocol which has been designed to provide protected cryptographic remote command-line access over untrusted networks. Its functionality breaks the rudimentary plaintext concepts like Telnet and encrypts both user information and session data to allow routers, firewalls and servers to be managed with administrative privileges.

Normally the SSH industry is working on TCP port 22 and the combination of a key exchange part of process with symmetric encryption to protect the management channel from eavesdropping or manipulation.

SSH is a system that enables privileged administrative access, so when it is provisioned in a widespread manner across an enterprise network it is creating a high-value attack vector. Accordingly, most consensus holds that SSH should only be accepted to authorized management stations and designated infrastructure assets and thus robust authentication mechanisms and extensive logging should be applied. In this way, single access for authorised administrators from known IP addresses is allowed to access critical systems. By segmenting and limiting SSH in this way the opportunities for lateral movement by adversaries are limited, and individual management actions can be traced for audit and forensic purposes.

The newly added Rule 1, which is named the "ssh rule," is the key administrative access control that is designed to enable safe remote management of the gateway. It explicitly allows SSH traffic (TCP port 22 traffic) from the "A-GUI" management station to the "A-GW" gateway interface. By making this the top rule in the Access Control Policy, this configuration gives priority to management traffic, so that the fact that later rules may impose a greater restriction on access will not prevent administrative access. The action is set to Accept with Log tracking enabled thereby providing a needed audit trail of all command-line access attempts and in line with established security best practices for monitoring privileged connections.

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 successful output of ping indicates that the network has been correctly configured and the firewall policy implemented correctly, allowing the administrative workstation two-way communication with the interface of the gateway. Specifically, the Command Prompt displays "A-GUI" (almost certainly the workstation at 10.1.1.201, given most earlier context) successfully receiving ICM - echo responses from the gateway at 10.1.1.1 with zero packet loss and a constant round - trip time of about 2 ms. The connectivity as observed supports the "gui ping to gw" rule (Rule 2) outlined in the policy, which clearly allows ICMP traffic. The provided network topology explains further the physical and logic path "A-GUI" resides upon the Management network (IntCP,10.1.1.0/24) and there "A-GUI" has "6-A-GUI (10.1.1.1) as a default gateway where it can route its traffic securely to other segments like the Domain Controller(S-DC) on IntSWA network (192.168.1.0/24) or the Child Domain Controller(L-CDC) on IntLCD network (192.168.2. The ping successful test is thus a building block of connectivity testing as it checks the Layer 3 routing and Layer 4 security policy enforcement before more complicated services like SSH or FTP are used.

```
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 successful start of the Secure Shell (SSH) session from the administrative workstation to the gateway at 10.1.1.1 is shown on the screenshot, which hence proves that the "ssh rule" we recently implemented is actively allowing traffic on TCP port 22. By running the command `ssh admin@10.1.1.1`, the client uses the standard "Trust On First Use" or TOFU security mechanism where the unknown host key fingerprint (ED25519) has to be explicitly accepted by the user before the establishment of a secure channel. Upon the user confirmation of the connection by typing "yes," the gateway's IP address is then permanently added to the client's `known_hosts` file and the session continues to display the configure legal banner ("This system is for authorized use only") followed by the password prompt. This sequence proves that the firewall policy is properly set up to allow remote management access, thus it successfully allows the application layer request to hit the gateway's authentication service.

Enhanced Security Implementation Through Advanced Features

Application Control and URL Filtering

Application Control and URL Filtering are building blocks of Next-Generation Firewall (NGFW) functionality that provide fine control and governance of the web enabled applications and Internet traffic that go beyond traditional port based security filtering capabilities. Contemporary threat actors routinely exploit legitimate applications and websites to support the execution of command-and-control communications and data exfiltration and dissemination efforts, application-layer security controls are indispensable for efficacious threat mitigation. Deploying such capabilities addresses salient security concerns such as shadow IT applications, productivity deficits due to non-business Internet consumption, compliance infractions due to unauthorized data transfers and vulnerability exposure to malicious or compromised sites.

Configuration Implementation Process

The application control and URL filtering blades are enabled as a result of a systematic configuration process starting with the activation of the blades on the security gateway objects. Within SmartConsole, it is navigated to the gateway properties and the software blades Application Control and URL Filtering are both enabled, thus ensuring the gateway has the necessary licensing and threat prevention capabilities. Subsequently, the access control policy layer will need to be configured to provide these features; this is done by right-clicking on the policy layer and then clicking "Edit Layer" and checking the applications and URL filtering check boxes.

The implementation provides various policy rules that deal with specific security requirements. A basic principle bans high-risk categories of applications, specifically anonymizers, proxy-avoidance services, peer-to-peer file-sharing services, and remote administration tools that have not obtained express permission to conduct business. The configuration of this rule states "Any" internal users as the source and Internet as destination, a "Anonymizer" and "P2P File Sharing" category is added in the "Services & Applications" field and an "Drop" action is applied. UserCheck notification is enabled to notify users about any policy violations.

For the purposes of productivity management, supplemental regulations put restrictions on access to social networking and entertainment websites during standard business hours for employees who do not hold executive positions. By combining Identity Awareness, these regulations define Access Role entities that represent specific user cohorts (e.g. "General_Staff" access role). The target domain is set to "Internet" and the Services & Applications attribute lists the relevant categories - as "Social Networking", "Streaming Media" and "Games" - and the respective action is "Drop". Embedded within this configuration is a UserCheck notification which explains the rationale of the policy. Such a methodology provides transparent security enforcement and at the same time keeps the user informed about the acceptable use policies.

Time-Based Access Control Policies

Temporal access - control mechanisms place time-bound restrictions on access to network resources and help to improve organizational security posture by limiting windows of time when resources may be exposed to a potential attack and ensuring that operational security protocols are implemented during business hours and workforce schedule. This capability supports a range of security scenarios, such as limiting non-essential access to the Internet to business hours in order to minimize the attack surface during after hours, preventing execution of sensitive operations during maintenance windows, enforcing compliance requirements for temporal separation of duties and managing bandwidth consumption during peak periods of operation.

Configuration Implementation Process

Within SmartConsole, one has to go to Object Management, click on Time Objects, and create new time definitions for: operational hours, such as a period called "Business_Hours" from 09:00 to 17:00-within weekdays (Monday to Friday), and date ranges, such as seasonal or project-specific restrictions. These time objects are then incorporated in the Access Control rules by activating the Time column in the rule base and linking the appropriate time objects with the designated rules.

The example of a practical implementation defines the restriction of general internet browsing to business hours for a standard employee population. The rule configuration states that the source is the "GeneralStaff" access role, the destination is the "Internet," the services are "HTTP" and "HTTPS," the Time field is populated with the "BusinessHours" time object and the action is "Accept." Complementarily, a deny rule is placed underneath where the parameters are the same except for the time restriction (ensuring that internet access outside business hours is explicitly blocked with the suitable logging for security monitoring).