

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

Student Name: Md Al Amin Sarkar Reday

Student ID: 2406207

MSc (Cybersecurity and Digital Forensics)

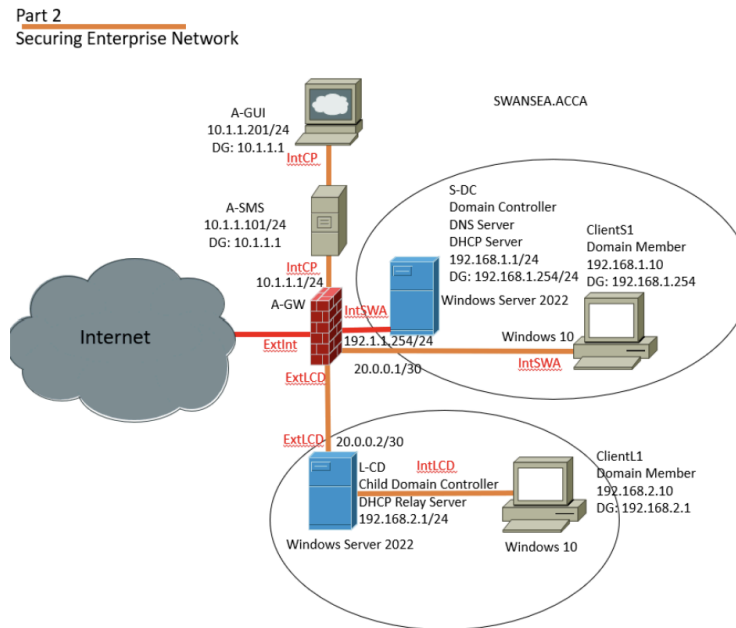
Enterprise Network Security

Module code: ACCA7032

Table of Content

Introduction To Topology.....	3
Task 1: Installation and Configuration.....	4
Configuring Network Settings.....	4
Installation of SmartConsole on A-GUI.....	5
Installing the Primary Security Management Server (A-SMS).....	6
Installation of the Check Point Gateway (A-GW).....	10
Running the First Time Wizard on the Security Gateway.....	11
Establishing Secure Internal Communication.....	15
Managing Licence.....	18
Attaching a Licence Using SmartUpdate.....	19
Update the Service Contracts.....	22
Generating a Licence Report.....	23
Task2 : Firewall Rules Configuration and Policy Implementation.....	24
Task 3: Enhanced Security Implementation Through Advanced Features.....	30

Introduction To Topology



This network uses a hybrid design combining a standard windows service environment with a specialized Check Point security layer. The topology is split into 2 main organizational sites: SWANSEA.ACCA and LONDON.SWANSEA.ACCA. These locations are connected via a point-to-point routed WAN connection through the 20.0.0.0/30 subnet that is considered the backbone for communication and resources.

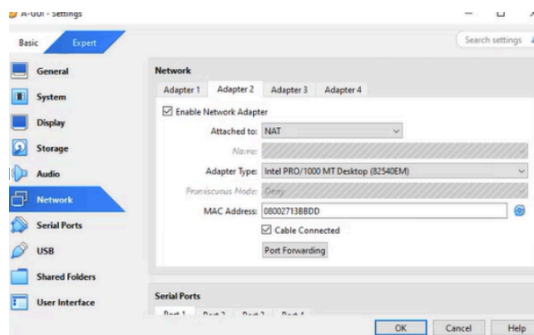
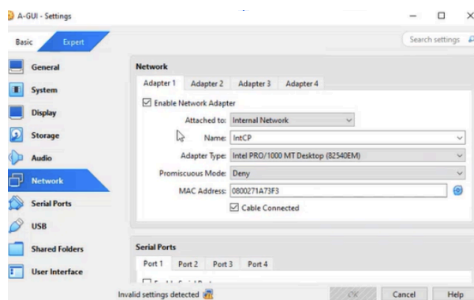
The main network and the main administrative domain are the SWANSEA.ACCA site. It contains the root Active directory Domain controller S-DC with the IP address 192.168.1.1/24. This server includes other basic services such as DNS, DHCP, and centralized identity management using Active Directory. A domain member workstation, ClientS1 (192.168.1.10), has also been located here. The LONDON.SWANSEA.ACCA site is a child domain and it has a supplemental domain controller, L-CD (192.168.2.1/24), configured as a DHCP relay agent, and its corresponding client, ClientL1 (192.168.2.10).

A major improvement to this design is the use of a Check Point security suite in an isolated management network segment, 10.1.1.0/24. This suite has three main components: the Security Management Server (A-SMS), 10.1.1.101, as the central point of management of security policies; the Security Gateway (A-GW) as the default gateway for the Swansea LAN, 192.168.1.254, for the purpose of inspection of communication; and the Administrative GUI workstation (A-GUI), 10.1.1.201, operating the Smart Console. This arrangement forms a

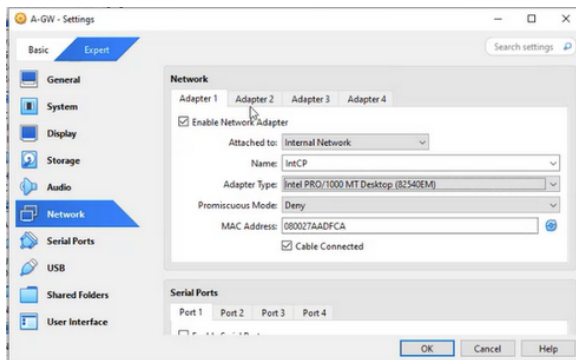
hub-and-spoke security architecture in which traffic to and from the internal networks must go through the security gateway to enforce security policies and check for threats.

Task 1: Installation and Configuration

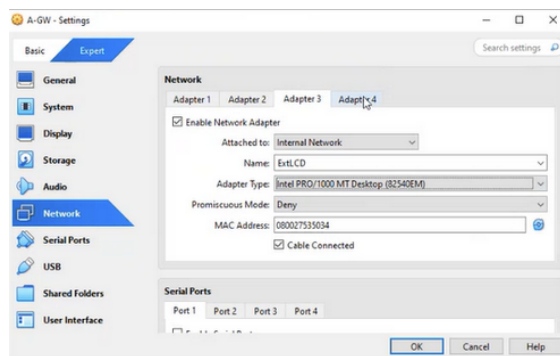
Configuring Network Settings



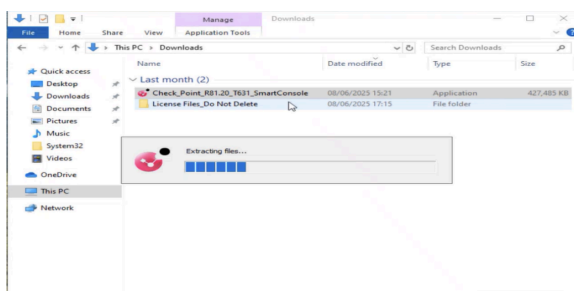
The basis of the Check Point lab environment is a deliberately segmented network environment, achieved by the virtual networking capabilities of Oracle VirtualBox. A key to such a design is the separation of the management layer from everything else using a dedicated virtual switch: so called IntCP. This secure network segment provides an interconnection between the administrative client (A-GUI), the central management server (A-SMS) and the enforcement gateway (A-GW) resulting in a trusted backbone for critical operations. All configuration commands, policy installations and system logs pass down this private channel, which provides administration integrity, segregating it from production-style data traffic. Furthermore, to serve the important purposes of maintenance, the A-GUI and A-SMS are fitted with other network adapters in NAT mode. These adapters provide a controlled access to the outside-internet to updates and threat intelligence feeds using the host machine connection to the maximum while maintaining the utmost isolation of the core lab environment.



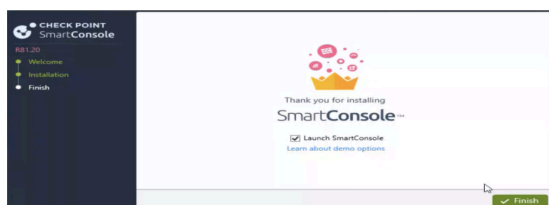
The Security Gateway (A-GW) is the core policy enforcement node, the design of which includes multiple network interfaces to replicate an enterprise environment with great accuracy. Alongside its dedicated management connection on the secure "IntCP" segment, the gateway also has three additional, each with its own specific function. One interface is configured using NAT creating a simulated route to the public internet. Another is on the 'IntSwa' network, this one carrying traffic for the internal users of the Swansea headquarters. A final adapter goes to the "ExtLCD" network to emulate the dedicated WAN from the London branch. This controlled separation of traffic flows using four portals allows the gateway to carefully control and secure access between the administrative realm and the spaces of the main corporate site, and the remote office and the untrusted external network.



Installation of SmartConsole on A-GUI

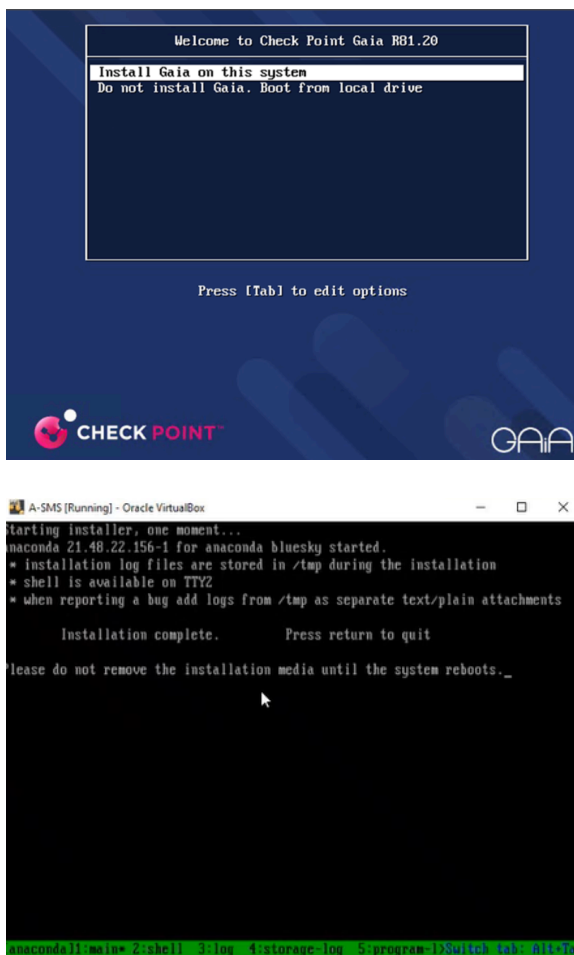


A series of screenshots are presented in order to visually depict the installation process of the SmartConsole management client on the A-GUI administrative computer. The journey starts as a result of the user starting the setup executable file from the Downloads folder. The first reaction that can be seen from the application is a progress bar dedicated to the extraction of the necessary installation files. This goes into another more detailed setup screen in which progress is measured at 15%, and is marked out by a marketing message

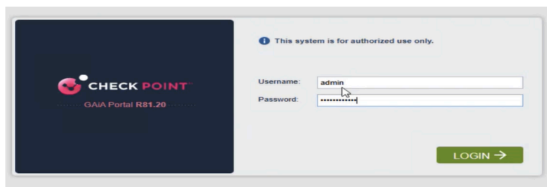


that includes "Efficient Automated Operations." The visual documentation ends up with a final successful screen, with it saying the setup process of SmartConsole R81.20 is complete. This last screen shows the workstation is now set up to be the center to perform its role as the central hub for security policy administration.

Installing the Primary Security Management Server (A-SMS)



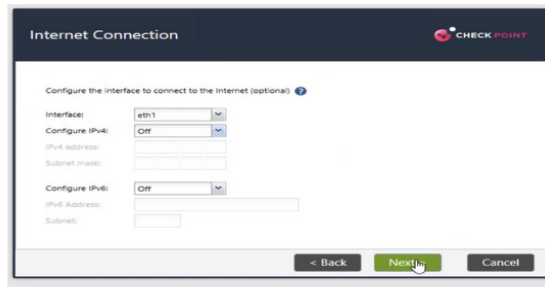
The process to install the Check Point Security Management Server (A-SMS) starts by starting the system from the Gaia R81.20 installation media. During the initial setup phase, the installer divides the 80 GB hard disk based on a predetermined scheme that includes dedicated space for the actual operating system, log files, swap memory and possible backups and/or upgrades in the future. It then automatically moves over all the required system files to these prepared partitions. The phase ends in a success notice which forces a system reboot in order to finalize the system installation and boot in the new Gaia OS.



CHECK POINT
 Gaia Portal R81.20

This system is for authorized use only.

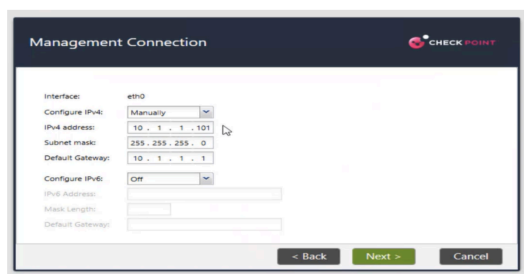
Username: admin
 Password:
 LOGIN →



Internet Connection

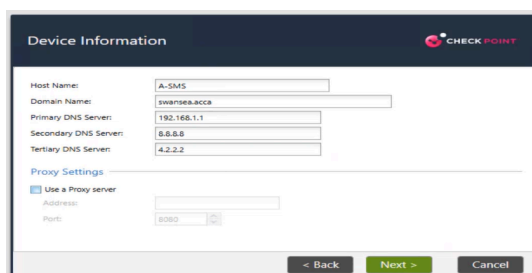
Configure the interface to connect to the Internet (optional)

Interface: eth1
 Configure IPv4: Off
 IPv4 address:
 Subnet mask:
 Configure IPv6: Off
 IPv6 Address:
 Subnet:
 < Back Next > Cancel



Management Connection

Interface: eth0
 Configure IPv4: Manually
 IPv4 address: 10 . 1 . 1 . 101
 Subnet mask: 255 . 255 . 255 . 0
 Default Gateway: 10 . 1 . 1 . 1
 Configure IPv6: Off
 IPv6 Address:
 Mask Length:
 Default Gateway:
 < Back Next > Cancel



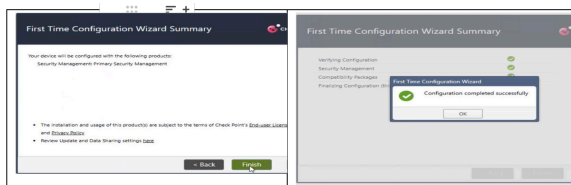
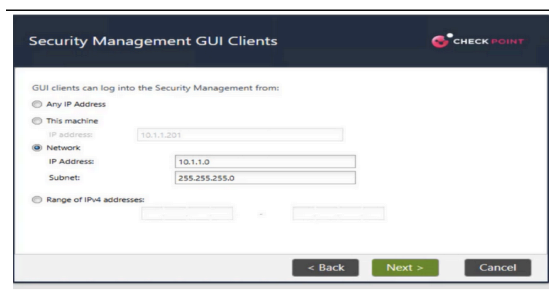
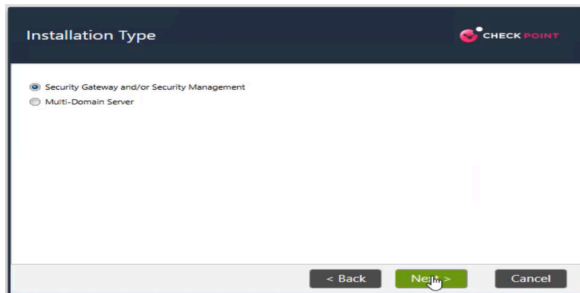
Device Information

Host Name: A-SMS
 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

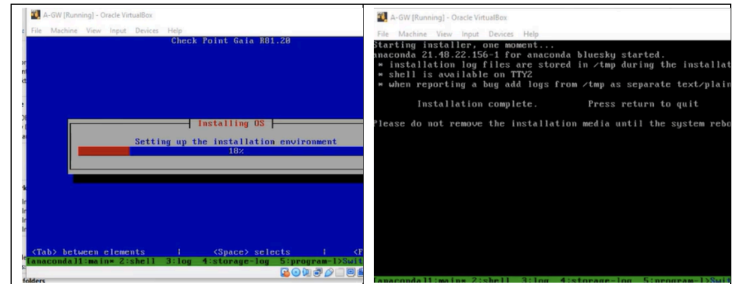
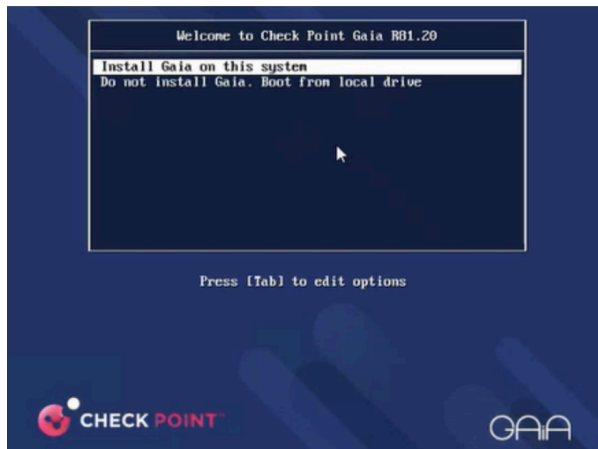
After the server is rebooted, the administrator logs into the Gaia Portal using a Web browser on the A-GUI workstation to start the First Time Configuration Wizard. An absolutely necessary task that is performed in this wizard is to manually assign network parameters to the primary management interface, eth0. static IP is 10.1.1.101, Mask is 255.255.255.0 and the gateway is 10.1.1.1 which places the server correctly on the isolated management network for the lab. The configuration of the secondary interface (eth1), which will be facing the internet is left for a future time. This step determines the network identity of the server which is created and then the server can work on the management plane and is now ready for further stages of configuration.



Taking the steps one by one through the First Time Configuration Wizard, the administrator establishes the necessary identity and role for the new Security Management Server. The device is called "A-SMS" and incorporated inside a domain called "swansea.acca." For name resolution to work, the DNS configuration is configured to point to the internal Domain Controller (192.168.1.1) for local name resolution, but also includes other public DNS servers that will resolve the name in case external query paths need to be used for external name resolution and services (updates). For the product installation, the simple "Security Gateway and/or Security Management" option is chosen, which is perfectly suited for the single-organization lab and avoids the sophisticated service-provider Multi-Domain Server type of architecture.

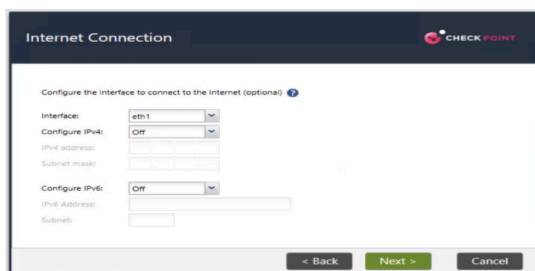
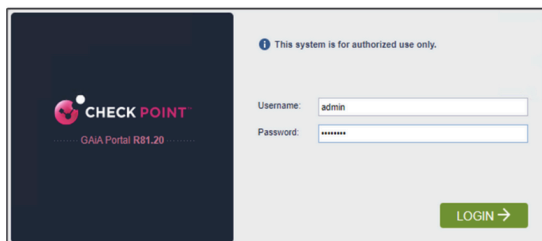
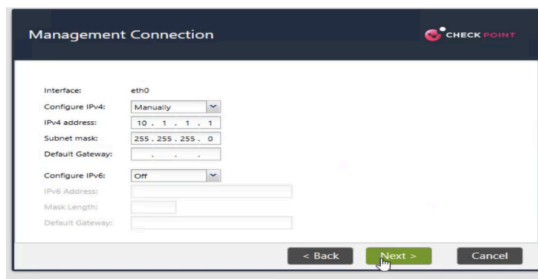
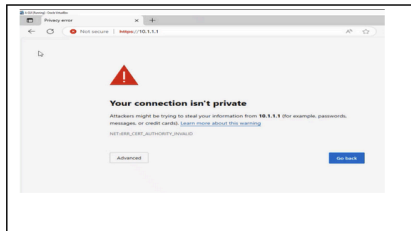
With the base identity set it creates a tighter security, by setting granular access controls. Administrative rights are limited to connections that come only from a designated management subnet 10.1.1.0/24 which essentially limits server access to trusted hosts such as the A-GUI client. The wizard finishes the run, showing a summary that is a validation of the configuration of a "Primary Security Management" server. Successful deployment then gets validated visually via the Gaia dashboard yielding the R81.20 system as operational and procedurally by a command line check of the status of the API server.

Installation of the Check Point Gateway (A-GW)



The Security Gateway (A-GW) setup starts by the virtual machine booting up from the Gaia R81.20 installation disc image. The administrator implements the "Install Gaia on this system", option from the initial first boot menu when it starts the OS deployment sequence. This installation is a standardized, automated process as indicated by a progressing status bar as the files are copied and configured. The phase ends with a prompt clearly saying "Installation complete" which instructs the user to type Enter. This action results in a system reboot which completes this basic stage in the gateway's configuration.

Running the First Time Wizard on the Security Gateway



The setup of the Security Gateway (A-GW) starts with the administrator using the browser of the management workstation to access the Gaia web portal by taking the initial self-signed certificate alert, to access the login screen. On the First Time Configuration Wizard, the network information of management interface (eth0) is checked as 10.1.1.1/24 so that it is on the proper segment to communicate with the management server. The configuration used for internet-facing interface (eth1) is delayed on purpose leaving its protocols disabled. The identity of the gateway is then designed, which receives the "A-GW" hostname, association with the "swansea.acca" domain and a DNS setup that prioritises the internal domain controller for local DNS resolution and keeps public DNS for backup purposes.



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

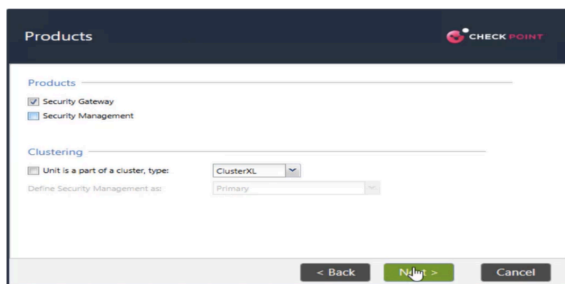


Dynamically Assigned IP

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

☐ Yes
☒ No

< Back Next > Cancel



Products

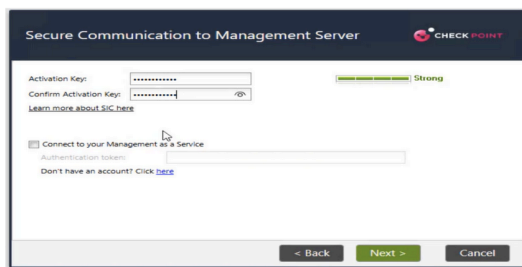
Products

☒ Security Gateway
☐ Security Management

Clustering

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

< Back Next > Cancel



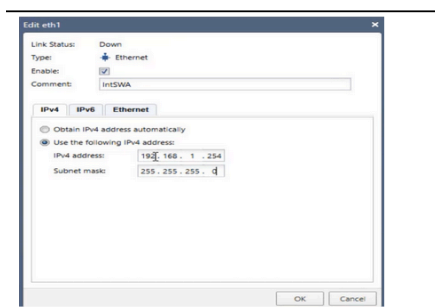
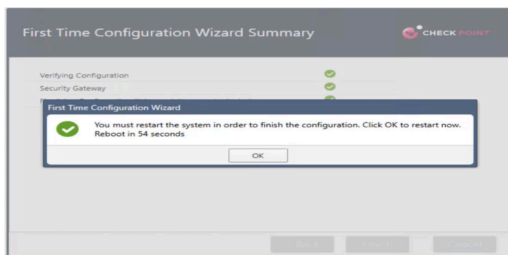
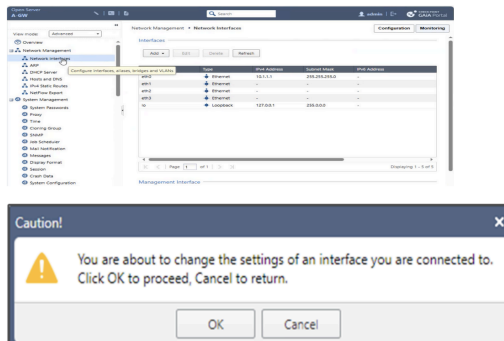
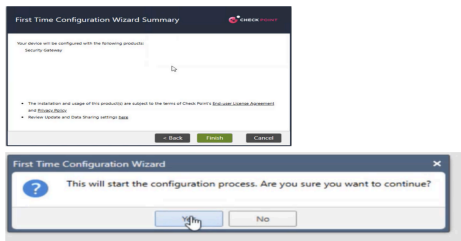
Secure Communication to Management Server

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

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

< Back Next > Cancel

Proceeding through the wizard, the operational purpose of the appliance is well defined by choosing "Security Gateway" and deselecting "Security Management," establishing its purpose as an enforcement point only. Clustering is not enabled and the gateway is configured to use a static IP address. The configuration ends in a vital path of starting Secure Internal Communication (SIC). By supplying the shared secret "Chkp!234" as the activation key a chain of trust is established which permits the central Management Server to authenticate itself, manage, and push policy updates to this gateway.



The last part of the configuration for the Security Gateway (A-GW) is done in the First Time Configuration Wizard. On the summary screen, the administrator makes a final check, that the role of the device is only listed under "Security Gateway", and presses "Finish" to push the configuration. This action causes an important system reboot in order to re-initiate the gateway fully on the new parameters. Once the appliance is up again the administrator logs back into the Gaia Portal to finish the network setup. Within the interface management section, the status of the management port (eth0) is reviewed showing it is active with the address 10.1.1.1. Attention then switches to the internal interface (eth1) which is enabled and configured using an IP 192.168.1.254. Scene description = "IntSWA", which is a descriptive comment added in this interface to formally associate it with the Swansea headquarters network segment.

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	-

Displaying 1 - 5 of 5

Network Management - IPv4 Static Routes

Add Edit Delete

Destination Address	Next Hop IP	Exit	Local Subnet	Outgoing Interface	Outgoing Interface	Flag	Comment
20.0.0.0	192.168.1.254	eth1	255.255.255.0	eth1	eth1	Y	

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:

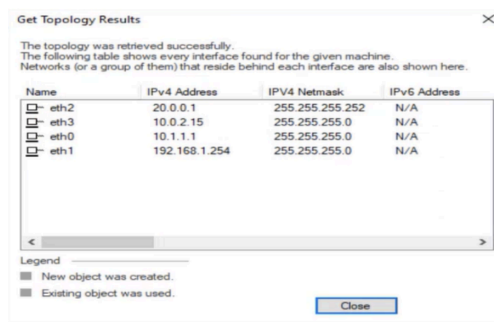
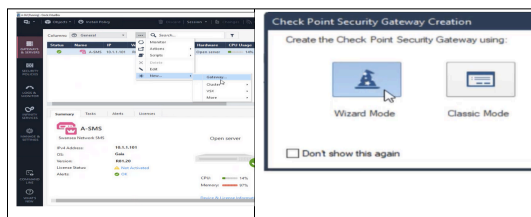
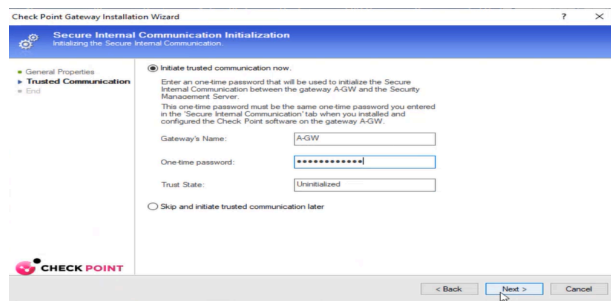
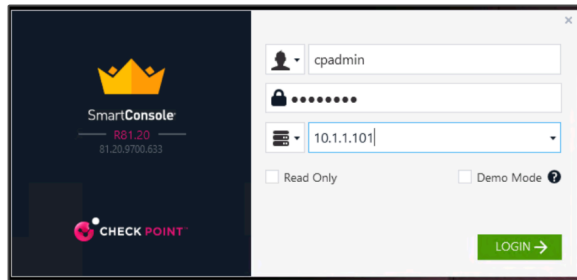
IPv4 address: 20 . 0 . 0 . 1

Subnet mask: 255 . 255 . 255 . 252

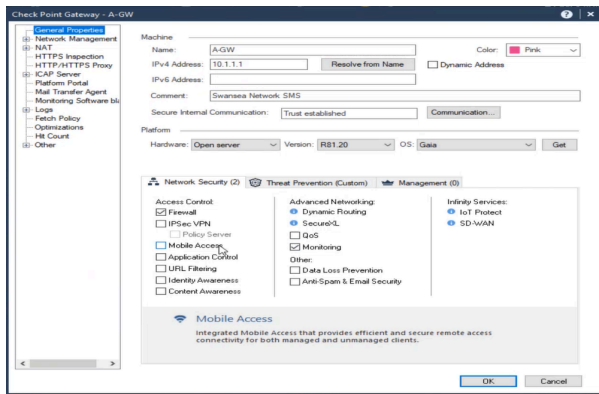
OK Cancel

In this final stage of the A-GW setup, the two last network interfaces are enabled and configured for their particular job. The administrator goes to the device settings for interface eth2, enabling this interface and setting the descriptive label to be "ExtLCD." A static IP configuration of 20.0.0.1/30 is made and this interface is granted as the end point for the point to point WAN link to the simulated London network. Attention then focuses on interface eth3 that is enabled and provided with the comment "ExtInt." One of its setups is configured to use a DHCP mechanism for automatic IPv4 address assignment to prepare it to use as a gateway, it is connected to an external or internet network. With such to apply configurations, the administrator terminates the session by logging out of the Gaia management portal and closing the web browser and the gateway's interface provisioning completes.

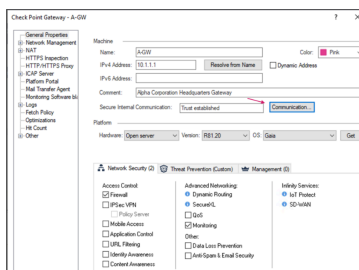
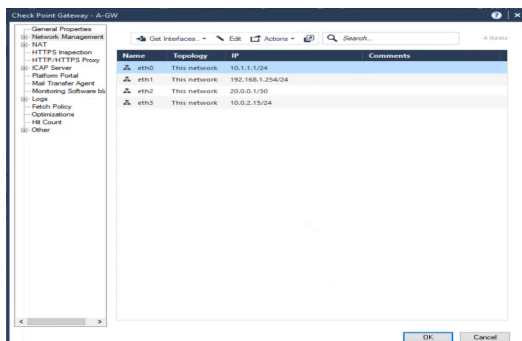
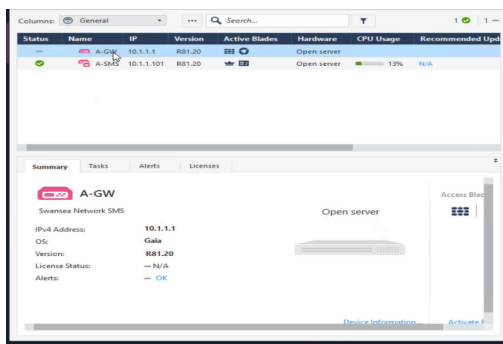
Establishing Secure Internal Communication

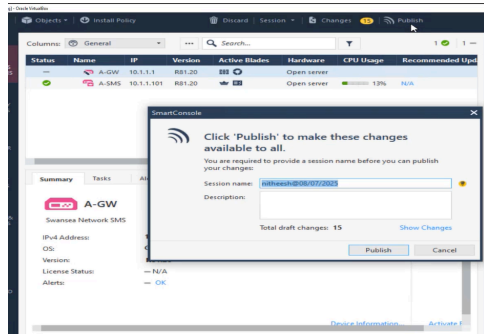
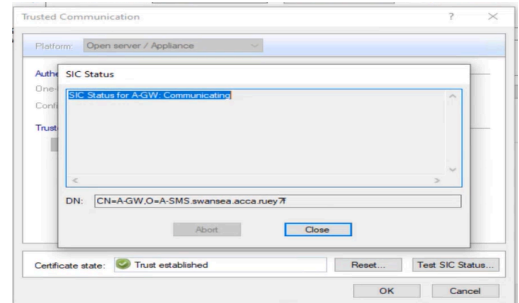
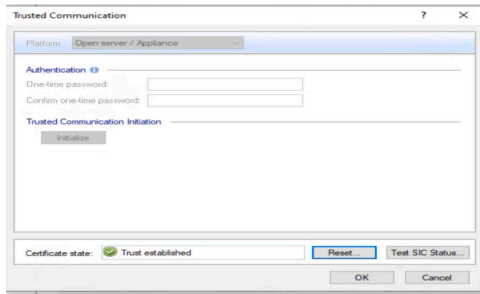


The process of merging Security Gateway into the controlled environment begins by opening the SmartConsole client from the administrator. Using the credentials of cpadmin application and connecting the management server at 10.1.1.101, access is granted. Within the management interface, the administrator starts the creation of a new gateway object using the very user-friendly Wizard Mode. The most important moment of this wizard is the creation of Secure Internal Communication (SIC). Using the name of the gateway A-GW and the Enter one-time password known in advance, connection a chain of trust between the management server and gateway is initiated. Upon successful authentication, SmartConsole dynamically imports gateway's topology network and displays a clear picture of all of its interfaces i.e. eth0 to eth3 with the address assigned to these interfaces for administrator's verification. Following the creation of the object, the capabilities of the gateway are extended by enabling the Mobile Access blade in the object's properties to make it ready for remote access VPN services. The now integrated A-GW is now a bona fide asset on the main dashboard. The procedure ends with a final check on the gateway's properties, in which the administrator verifies the proper identification information and, most importantly, is able to see the final state of "Trust established" for Secure Internal Communication, indicating the successful addition to the security fabric.



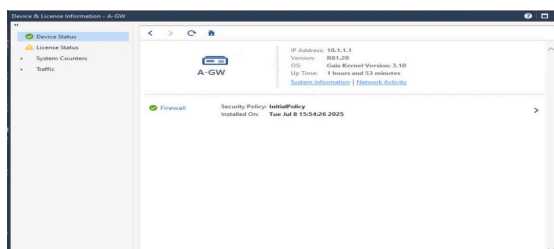
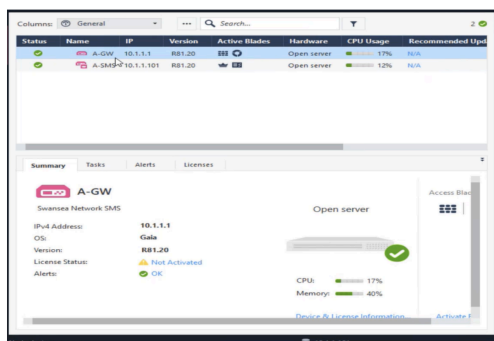
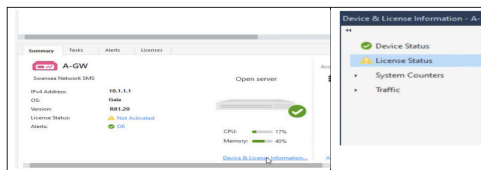
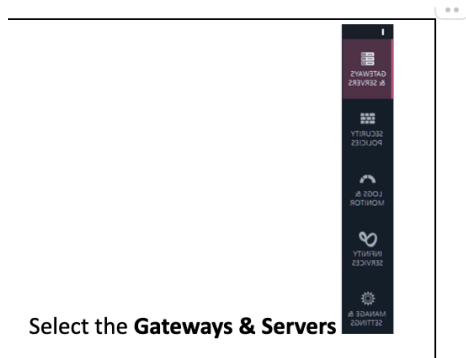
With the gateway object created, it is now time to enlarge the object's functionality. The administrator goes to the properties of the gateway to activate the Mobile Access blade which provisions the system for the secure remote access VPN services. Subsequently, the network topology view in SmartConsole is updated, and it shows a verified four interfaces (eth0 to eth3) and their associated IP network. The newly added A-GW becomes a visible asset on the main overview of the console, with the summary details to its success an attestation to its successful integration. The procedure ends with a final look at the gateway's configuration, in which the administrator checks the identifying information is correct and, most importantly, can check the Secure Internal Communication status is "Trust established," with the gateway successfully enrolled in the centrally managed security infrastructure.





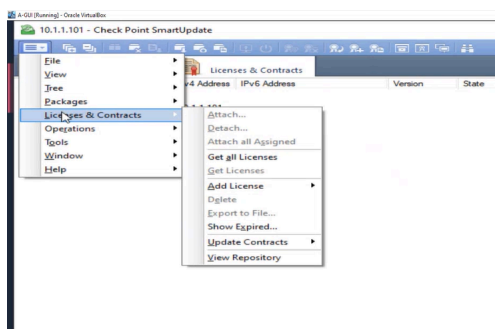
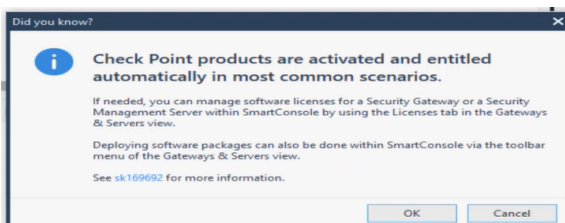
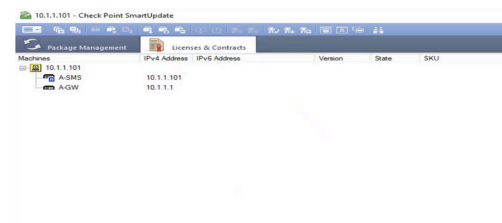
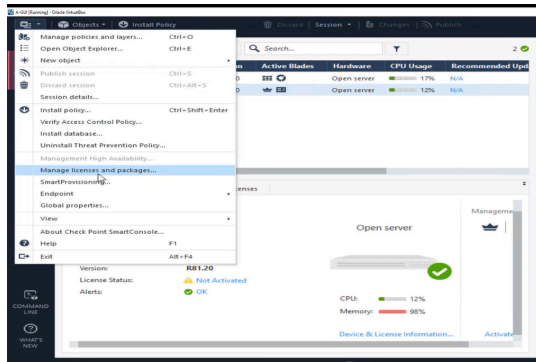
The images illustrate the final steps to check and complete the Security Gateway setup in SmartConsole with the final step of confirming the link of the Secure Internal Communication (SIC). The administrator opens up "Trusted Communication" window to view "Trust established" status with a green check. For added assurance the "Test SIC Status" button is clicked which comes back with the message "SIC Status for A-GW: Communicating" which indicates a secure communication channel is active. To finish the job, the administrator closes the verification dialogs and clicks "Publish" on the toolbar. This saves the new gateway and all the settings associated with it to the central database in the management server.

Managing Licence

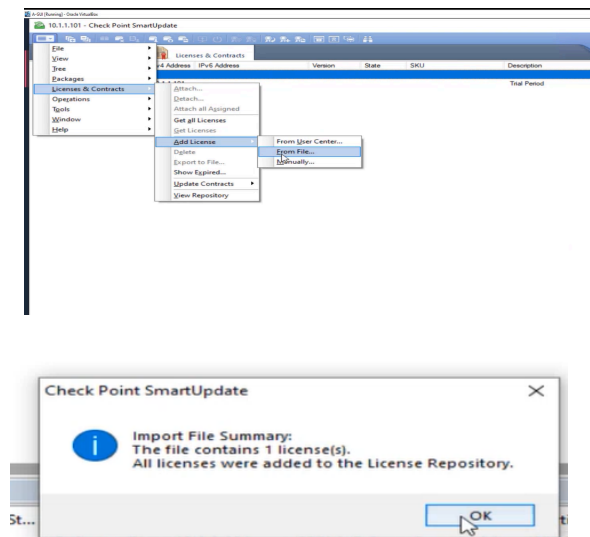


The following screenshots take the reader through the conclusive verification and commitment stage for the Security Gateway configuration in the SmartConsole environment, focusing on the Secure Internal Communication (SIC) link. The administrator does the validation by going to the "Trusted Communication" dialog box. Here, a positive "Trust established" status is confirmed that is visually reinforced by a green checkmark icon. An extra layer of verification is provided by selecting the "Test SIC Status" option that generates a responsive confirmation "SIC Status for A-GW: Communicating". This message gives definitive proof that there is a secure operational channel between the management server and the gateway. The process is completed by dismissing the open dialog boxes, and making a commit action by clicking on the "Publish" button on the toolbar, which permanently writes the new gateway's configuration into the management repository.

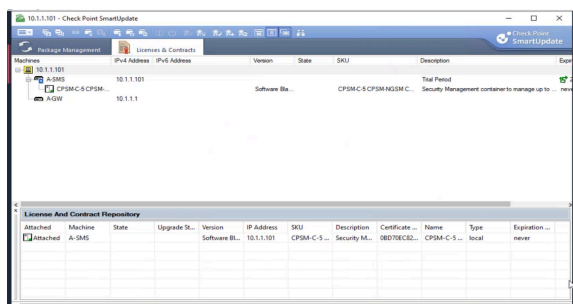
Attaching a Licence Using SmartUpdate



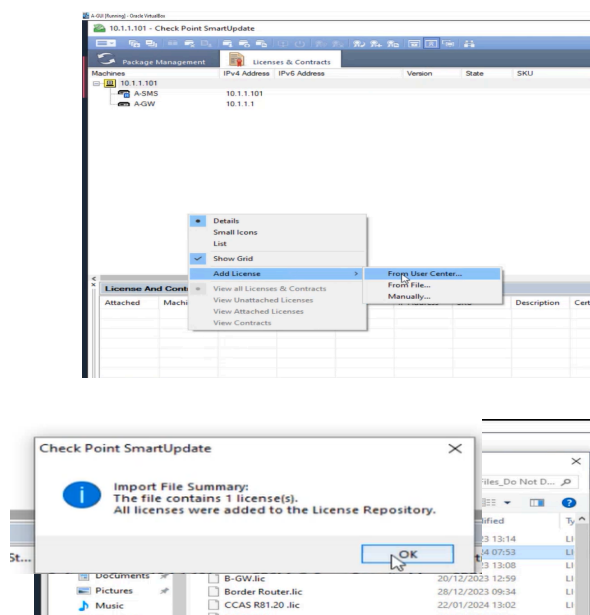
To begin licenses management the administrator logs in to SmartConsole and by using the main menu opens the "Manage licenses and packages" utility. After closing the informational pop-up about the automatic activation of Check Point, the SmartUpdate window will open displaying a tree of all the managed devices such as the A-SMS server and A-GW gateway. From here the administrator goes to the "Licenses & Contracts" menu and selects "View Repository." This opens the central repository pane in which all software licenses get stored.

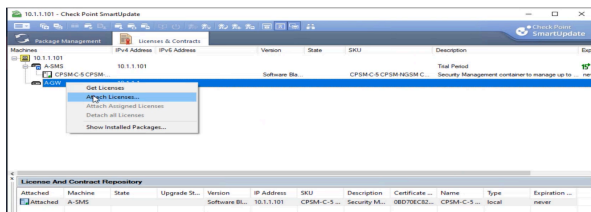


Next, the administrator wants to add a new license so he right-clicks inside the repository pane and selects "Add License > From File". This opens a file browser to browse to and upload the license file from the local computer. After you successfully upload, you get a confirm pop up and it says the license was found and added to the repository. When you click on "OK" the message closes and the import is finished and the license is ready to be assigned to a device.

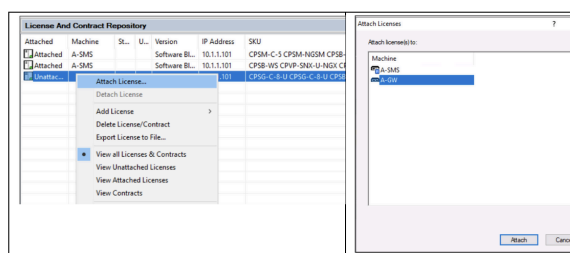


Completing the license assignment is a matter of importing the file via SmartUpdate interface. The administrator goes to the License & Contracts repository area, by right-clicking and selecting the option "Add License > From File." This opens a system file browser, in which the specific license file (e.g. A-GW.lic) is found and selected. Uploading the file provides an immediate response of a confirmation dialog saying that the license is successfully integrated into the central repository. Final verification is done in the main view of SmartUpdate, the repository pane should now list the new license with its status displayed to "Attached." This is the license correctly bound to the target appliance (to which A-SMS management server, for example) and is operational, often indicated by an expiration date that is listed as "never" for a perpetual license



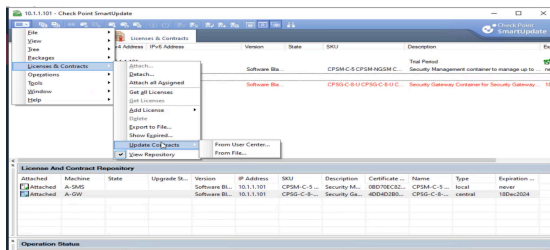
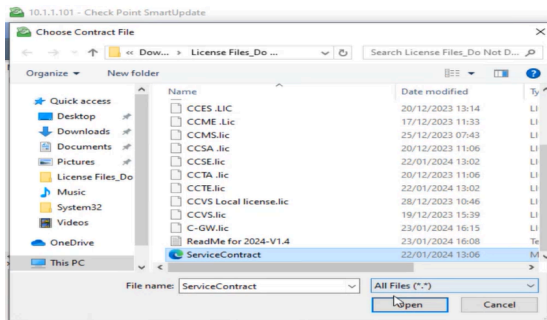
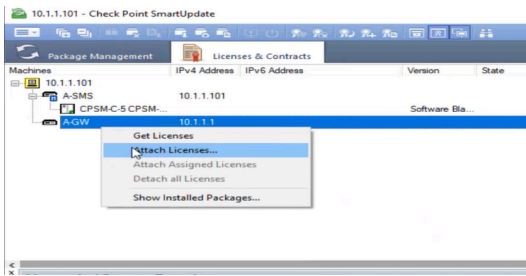


License And Contract Repository									
Attached	Machine	State	Upgrade St...	Version	IP Address	SKU	Description	Certificate ...	Name
Attached	A-SMS			Software Bl...	10.1.1.101	CPSM-C-5 CPSM-NGSM CPSB-WK...	Security Management container to manage up to		
Attached	A-SMS			Software Bl...	10.1.1.101	CPSB-W5 CPVP-SND-U-NGX CPSB-S...	Web Security blade, SSL Network Extender for un		
Attached	A-GW			Software Bl...	10.1.1.101	CPSG-C-8-U CPSG-C-8-U CPSB-FW...	Security Gateway Container for Security Gateway		



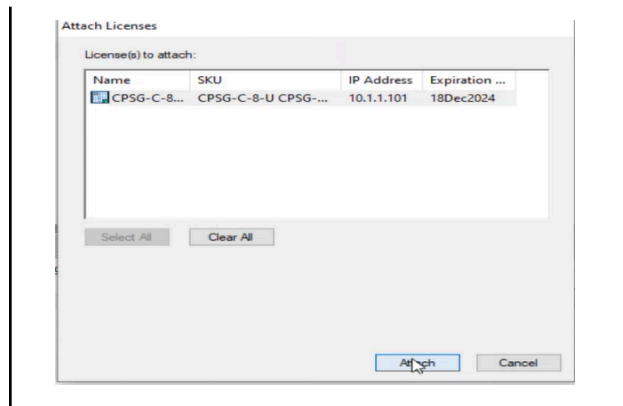
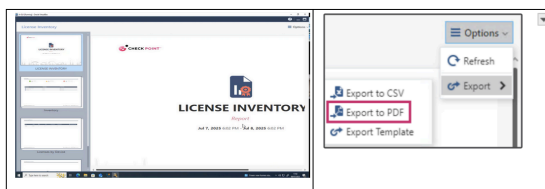
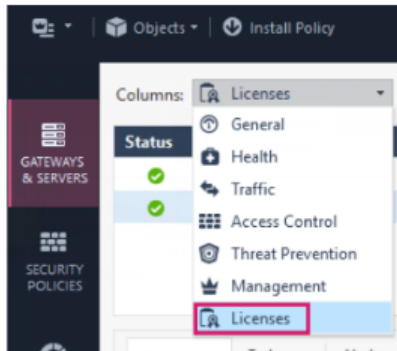
Centralization of license administration is done within the interface of Check Point SmartUpdate, through its "Licenses & Contracts" section. Here, in hierarchical overview are managed network objects, including the Security Management Server (A-SMS) and the Security Gateway (A-GW). Licensing can be done in two ways: By right-clicking on a particular appliance (such as the A-GW) and selecting the "Attach the licenses to the device" option. Via the option or through selection of an unattached license from the repository pane and assigning it a target device using the attachment dialog. The successful result of this is visually confirmed in the view on repository, where the status of the relevant licenses is updated to "Attached" to confirm that the software rights for the management server and gateway have been well bound and operational.

Update the Service Contracts.



The illustrated steps take you through the process of managing licenses and support contracts in SmartUpdate interface. The process starts in the "Licenses & Contracts" tab, where the hierarchy of the network is shown. In this case, the administrator chooses the security gateway A-GW and triggers license attachment using the right click "Attach Licenses..." option. To update contract entitlements, the user goes to the "Licenses & Contracts" main menu and clicks on "Update Contracts." This poses a choice between getting the updates directly from Check Point's online User Center, or from a file stored in your house. When you have chosen to update locally, a file browser "Choose Contract File" is displayed. The user goes to the directory holding license files, creates a list of relevant contracts (for example "ServiceContract") and clicks "Open" to complete the import into the repository.

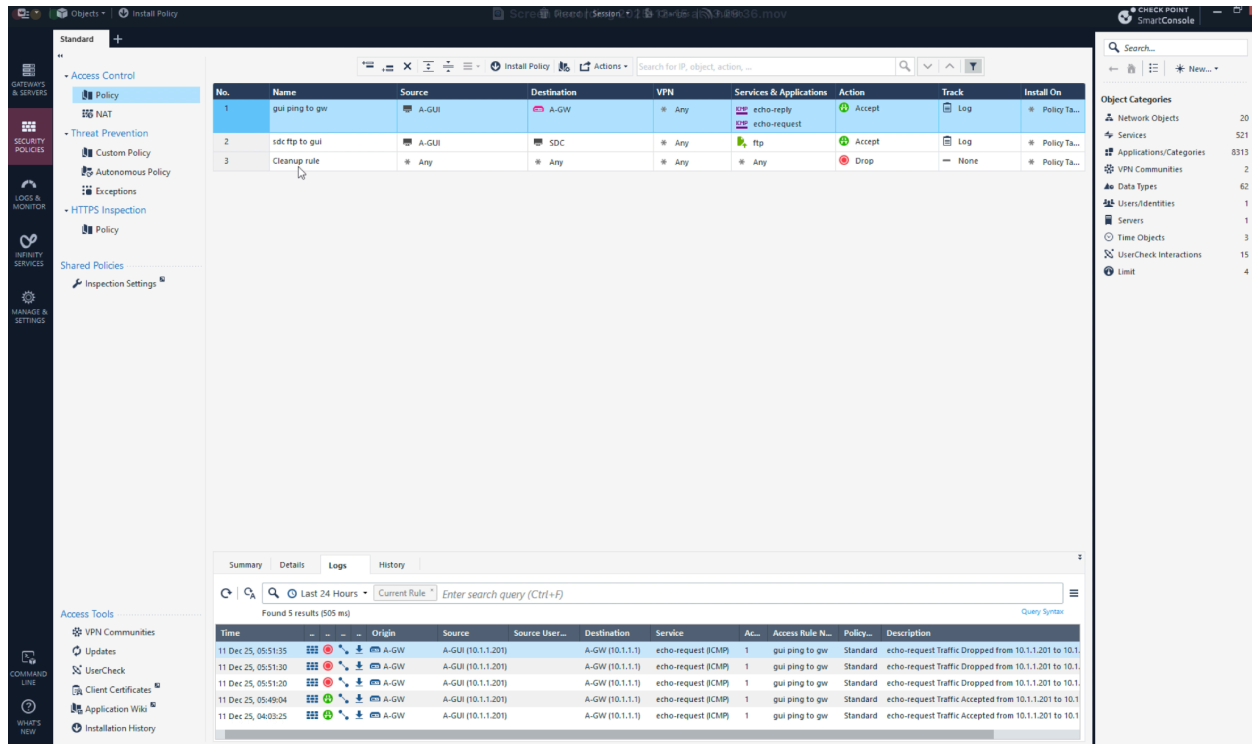
Generating a Licence Report



License management in Check Point SmartConsole starts with the personalization of the management view. By introducing the "Licenses" column to the "Gateways & Servers" dashboard, administrators can view vital information such as the "CK" and "SKU" status which reveals the presence of any unlicensed devices such as the A-GW gateway. For good record-keeping, an extensive "License Inventory" report is generated through the "Actions" menu and saved as a PDF document. To resolve the licensing gap the administrator follows the attachment procedure, dissipated in "Attach License" window where the desirable license is selected and applied with the target appliance with a press of the "Attach" button.

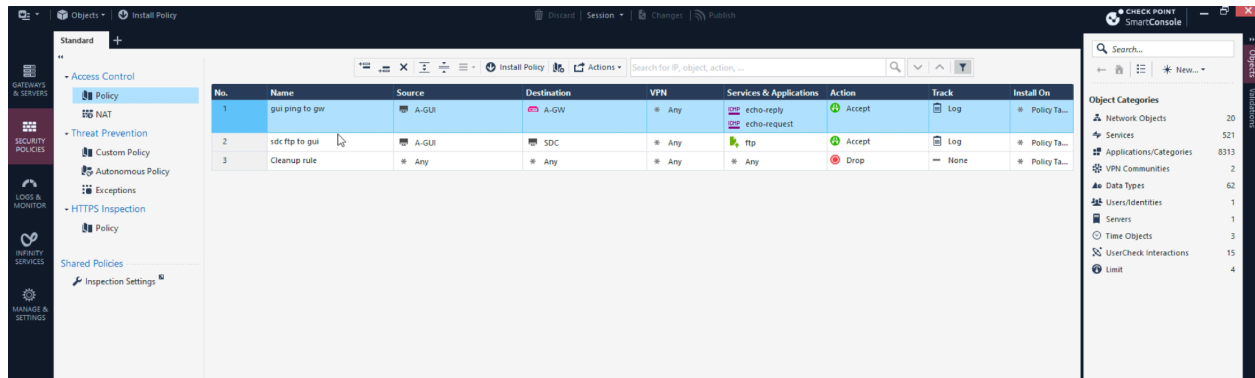
Task2 : Firewall Rules Configuration and Policy Implementation

Firewall Rules Configuration and Enterprise Security Policy Implementation



The image shows the Check Point SmartConsole, which is a unified management portal, bringing the configuration of policies, defining objects, and real-time monitoring into a coherent work space. This is designed to simplify the role of the security administrator by giving one comprehensive view. Navigation is supported by the left-hand sidebar which provide direct links into key areas such as Gateways & Servers, Security Policies and Logs & Monitor. At the center of the interface is the Security Policy editor which is the Access Control layer. An ordered rulebase is provided here which decides how the traffic is to be handled. Visible in the example are permit rules for ICMP and FTP traffic culminating in a final Cleanup rule, which denies all remaining packets - and represents a "positive security model" in which only explicitly authorized communication is permitted.

Every rule is constructed with the use of particular objects and services, the actions are predefined as Accept or Drop and the logging is provided for auditability. The preparation of these sorts of policies is an intuitive and visual process. Administrators can drag items from the object library directly into the cells of a rule instantaneously changing the parameters of the rule. After editing configurations, it is necessary to click the Install Policy button to make final configurations. This action builds the rulebase and moves it to the enforcement points, which means that the security logic that is defined will be actively applied throughout the network.



ICMP Configuration

The image shows the Check Point SmartConsole, which is a unified management portal, bringing the configuration of policies, defining objects, and real-time monitoring into a coherent work space. This is designed to simplify the role of the security administrator by giving one comprehensive view. Navigation is supported by the left-hand sidebar which provide direct links into key areas such as Gateways & Servers, Security Policies and Logs & Monitor.

At the center of the interface is the Security Policy editor which is the Access Control layer. An ordered rulebase is provided here which decides how the traffic is to be handled. Visible in the example are permit rules for ICMP and FTP traffic culminating in a final Cleanup rule, which denies all remaining packets - and represents a "positive security model" in which only explicitly authorized communication is permitted. Every rule is constructed with the use of particular objects and services, the actions are predefined as Accept or Drop and the logging is provided for auditability. The preparation of these sorts of policies is an intuitive and visual process. Administrators can drag items from the object library directly into the cells of a rule instantaneously changing the parameters of the rule.

After editing configurations, it is necessary to click the Install Policy button to make final configurations. This action builds the rulebase and moves it to the enforcement points, which means that the security logic that is defined will be actively applied throughout the network.

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	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...

FTP is a basic network protocol used for file exchange, and that works on a client-server basis. It uses two different TCP channels: control connection (port 21) to control and data connection (quite often at port 20) to transfer file contents. This dual-socket architecture enables certified file management on distant servers and secures its historical past as an data exchange within the enterprise setting.

Despite its usefulness, FTP has several major security risks because it doesn't contain any native encryption methods. All transmissions, including passwords and data transits in cleartext and are therefore exposed to interception. For this reason, it is highly recommended in modern security advice to replace FTP with other secure protocols such as SFTP or FTPS. When used because of legacy operational requirements - for example for a specific internal application - access needs to be strictly limited. This includes limiting the usage of FTP traffic to specific source and destination hosts on trusted network segments so that there is less potential for exploiting such vulnerabilities.

Configuring this restricted access in Check Point SmartConsole is the creation of a carefully-devised firewall rule. For example, this rule "sdc ftp to gui" would be built by specifying the authorized source client ("A-GUI") and destination server ("SDC"). The "ftp" service is applied to the rule, so the firewall knows how to intelligently inspect the control session, and keeps track of the data connections, dynamically. The action of the rule is set to "Accept" and the logging is enabled. This provides a critical audit trail and allows security teams to monitor for unauthorized attempts to transfer data or exfiltrate data.

SSH Access Rule

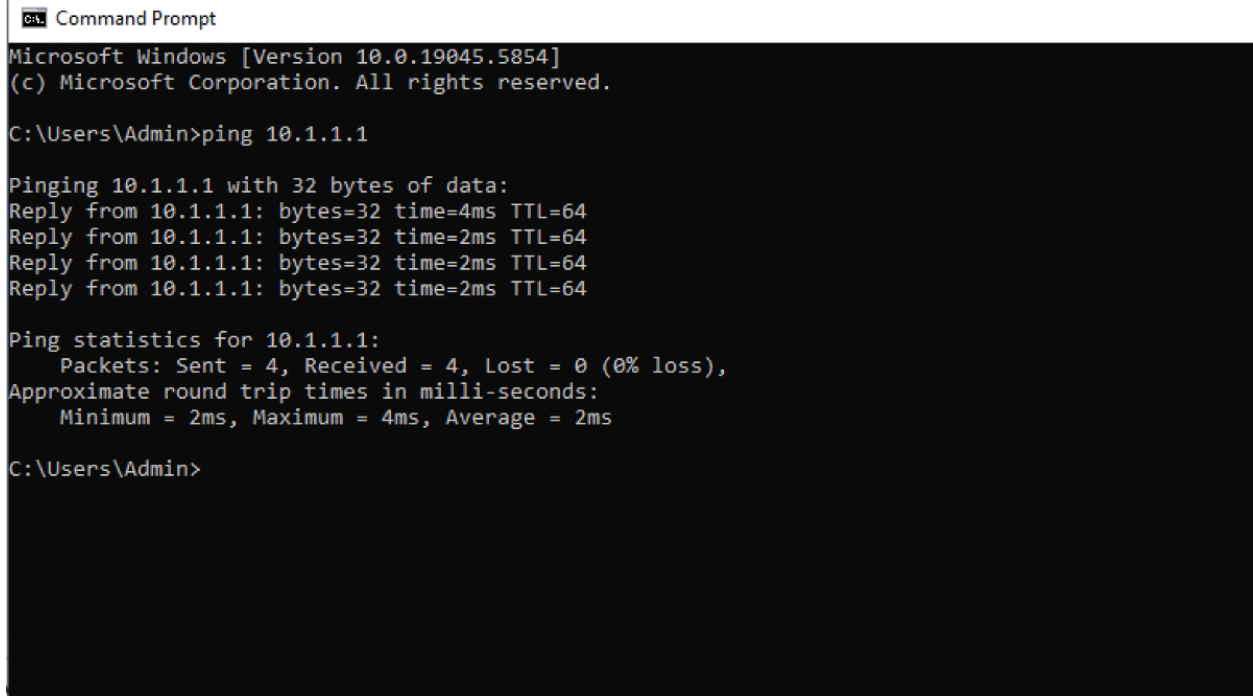
No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	ssh rule	A-GUI	A-GW	* Any	ssh	Accept	Log	* Policy...
2	gui ping to gw	A-GUI	A-GW	* Any	echo-reply echo-request	Accept	Log	* Policy Ta...
3	sdcc ftp to gui	A-GUI	SDC	* Any	ftp	Accept	Log	* Policy Ta...
4	Cleanup rule	* Any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

Secure Shell (SSH) is a basic encryption protocol for secure and remote administration that replaces insecure and plaintext options. By listening on TCP port 22 and using robust encryption systems to protect logical connections SSH protects the authentication process and then protects all subsequent commands providing in this way you can secure your network infrastructure operation on potentially hostile networks.

The powerful nature of ssh access requires it to be carefully restricted in an enterprise. Allowing it to be so broadly does create a large attack surface. Therefore, security best practices require SSH to be restricted to dedicated management subnets and specific hosts that are used to provide administration, and to be required to be strong via authentication. This segmentation limits the ability of an attacker to pivot with compromised credentials and all privileged access is logged to be held accountable and for forensic analysis.

The governing of this principle is shown in Rule 1, which is named ssh rule. This access control entry is designed to only allow SSH communications from the "A-GUI" administrative client to the "A-GW" security gateway. Its location as the first rule in the Access Control Policy ensures that administrative connectivity is ensured regardless of more general deny rules below it. Configured with an Accept action and Log tracking, the rule allows the visibility so important in order to control all the interactions on the command line with the gateway.

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 positive result received from the ping command is a good proof that the underlying network architecture and respective firewall policy have been implemented correctly. The output as the Command Prompt records the event is major success, administrative workstation "A-GUI" (working with IP address 10.1.1.201) is exchanging ICMP echo messages with gateway interface (10.1.1.1). The connection is shown as being stable even zero packet loss and a constant latency of about 2 milliseconds. This successful exchange is a direct validation of the functionality of the dedicated firewall rule, "gui ping to gw" (Rule 2) which was written specifically to explicitly authorize this type of diagnostic ICMP traffic.

The attached network topology adds your data flow some much needed context. It shows that A-GUI is on the isolated segment of the management network (IntCP, 10.1.1.0/24) and uses A-GW as a default gateway. This configuration allows A-GUI to securely access other important areas on the network such as the primary Domain Controller (S-DC) of the IntSWA network or the Child Domain Controller (L-CD) through the point-to-point WAN connection. Therefore, there is nothing trivial about this simple ping test which serves as a base level check for both the Layer 3 IP routing and Layer 4 security policy enforcement. Establishing this base connectivity is an important pre-requisite before administrators test and place their trust on more complex, application-layer services, such as SSH or FTP.

```
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 image shows a successful establishment of a Secure Shell session initiated from the administrative console to the management IP of the gateway; 10.1.1.1. This action confirms that the lately configured "ssh rule" found in the firewall is actually enforcing policy, allowing the traversal of the planned traffic on the selected TCP-port 22. The sequence Connect starts with the client making the `ssh admin@10.1.1.1` command which presents a typical "Trust On First Use" security dialog. Here, the administrator is required to place manual verification to accept the ED25519 host key fingerprint of the gateway. Upon confirming "yes" the identity of the gateway is written to the client's `known_hosts` file for future sessions. The secure channel is then opened to show the authorized use banner of the system followed by the authentication prompt. This flow gives definitive evidence that the firewall rule is correctly processing the requests at the application layer and is letting through the management traffic towards the SSH service of the gateway.

Task 3: Enhanced Security Implementation Through Advanced Features

Application Control and URL Filtering are the intelligent application layer enforcement aspects of a Next-Generation Firewall. They bring important visibility and rule of the actual software and web that runs through the network, responding to the evolution of the threats that use trusted services. Their deployment helps to address a range of risks to an organization ranging from data loss by an insider to compliance failures to penetration by malicious web content.

Configuration Implementation:

Activation is a two stage, action-based process. First of all, respective software blades are provisioned onto the enforcement gateways, which is a step that requires valid licensing. Subsequently, the administrative policy layer itself has to be modified in order to process the application and URL data, which is done in the properties of the policy layer in SmartConsole.

The granular visibility of policy construction is leveraged. A general ground rule security measure is usually put in place to block high-risk application types (such as anonymizers and peer-to-peer networks) from any internal source to the internet. This rule uses a "Drop" action that is complemented with UserCheck, with a protective and educative purpose. Further refinement is introduced by Identity Awareness where rules can be applied to defined user groups to thin out the use of non-business applications such as social media to align network usage with acceptable use policies using transparent, message-based blocking.

Access Control Policies Based on Time:

Temporal restrictions bring a dynamic aspect of enforcement of policy within the context. By assigning access permissions to specific time intervals, organizations can strategically shrink their attack surface, apply shift-based policies, and make sure they are doing exactly what they want them to do at the specific time.

Configuration Implementation

The process is grounded in the time objects created by which we will enforce ourselves into reusable objects, namely hours, days or seasonal periods. In the Access Control rulebase, these objects are used for rules to which they apply. A classic implementation is the complementary rule pair for user internet access - the first rule allows web traffic for staff role only during the defined "Business_Hours" time object. The second, catch-all rule with the same parameters but without the time constraint then rejects access during any other time. This architecture provides that a positive security model is established temporally with clear allow and deny periods with full logging for audit and incident response.

