

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

MSc (Cybersecurity and Digital Forensics)

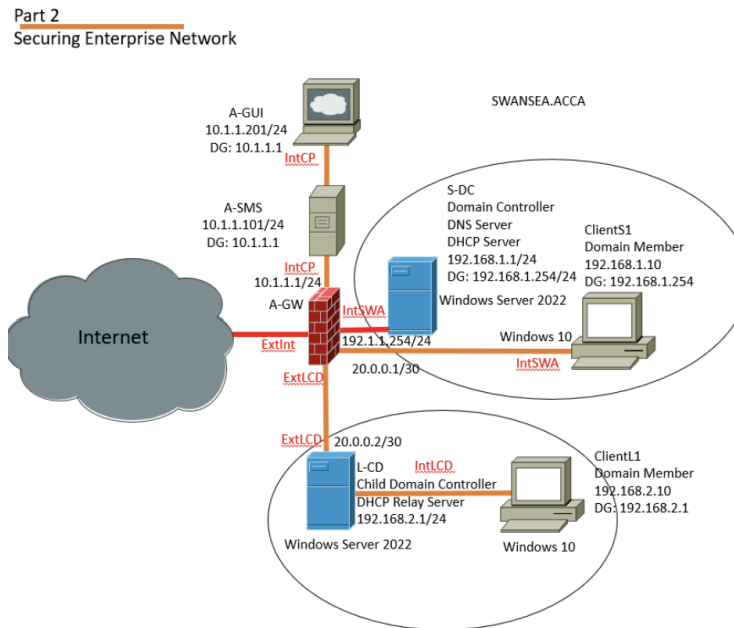
Enterprise Network Security

Module code: ACCA7032

Table of Content

Introduction.....	3
GAIA Appliances Overview.....	4
Installation and Configuration of A-GW, A-SMS, A-GUI.....	5
Configuring Network Settings.....	5
Installation of SmartConsole on A-GUI.....	6
Installing the Primary Security Management Server (A-SMS).....	8
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.....	17
Attaching a Licence Using SmartUpdate.....	18
Update the Service Contracts.....	21
Generating a Licence Report.....	22
Firewall Rules Configuration and Enterprise Security Policy Implementation.....	23
Configuring ICMP Policy.....	24
Configuring FTP Policy.....	25
Configuring SSH Policy.....	26
Validating the policy.....	27
Enhanced Security Implementation Through Advanced Check Point Features.....	29

Introduction



The enterprise network being considered represents the hybrid architectural model where a traditional Windows-based service infrastructure is combined with an enforcement layer of Check Point security. As shown in the topology provided, the environment is divided into two main organisational sites, which are SWANSEA.ACCA and LONDON.SWANSEA.ACCA. These sites are interconnected using a dedicated point-to-point routed connection using the 20.0.0.0/30 subnet to provide a wide-area network (WAN) backbone to enable inter-site communication and sharing of resources. The SWANSEA.ACCA site is the network core and main administrative domain. It has the root Active Directory Domain Controller (S-DC) that is configured with the IP address 192.168.1.1/24.

This server plays a number of roles that are critical to an organisation, 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). A client workstation, ClientS1 (192.168.1.10) is deployed as a member of this subnet's domain. Conversely, the LONDON.SWANSEA.ACCA site is a child domain, where there was a supplementary domain controller (L-CD, 192.168.2.1/24) with the configuration of 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 in a dedicated management network segment (10.1.1.0/24).

This suite consists of three main appliances the Security Management Server (A-SMS, 10.1.1.101) which is the central policy repository and administrative hub, the Security Gateway

(A-GW, 192.1.1.254) which is situated as the default gateway (192.168.1.254) for the Swansea LAN, to perform traffic inspection, and the Administrative Graphical User Interface workstation (A-GUI, 10.1.1.201), from which the Smart Console management application is operated. This topology provides an effective implementation of a hub-and-spoke security model, in which all traffic going to or coming from the secure internal networks is forced to pass through the security gateway, to provide a full set of policies and threat inspections.

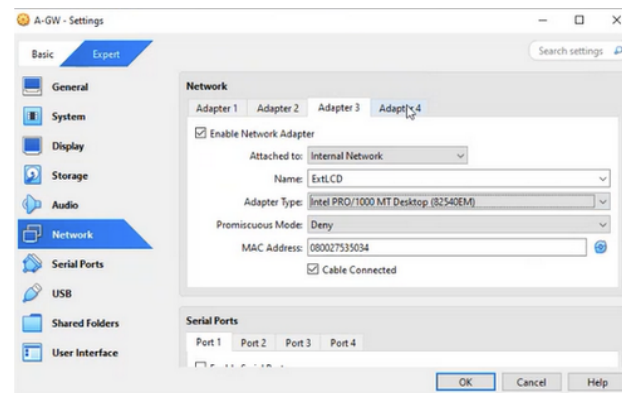
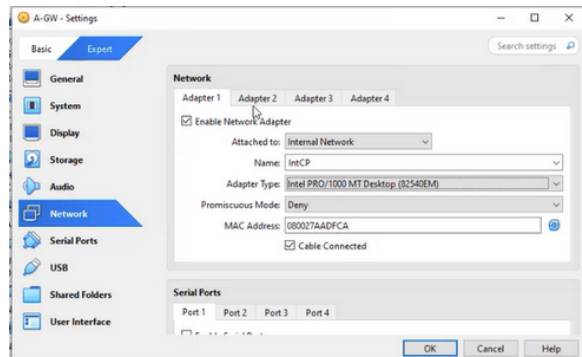
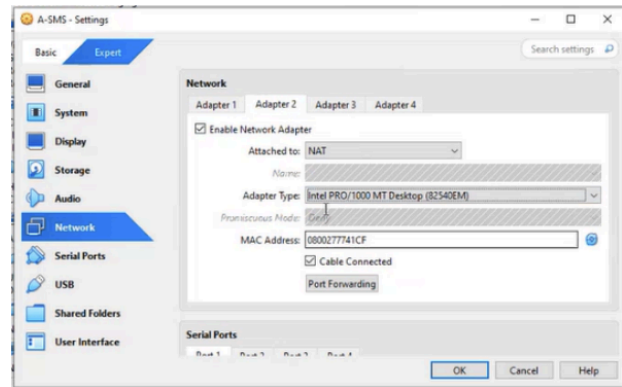
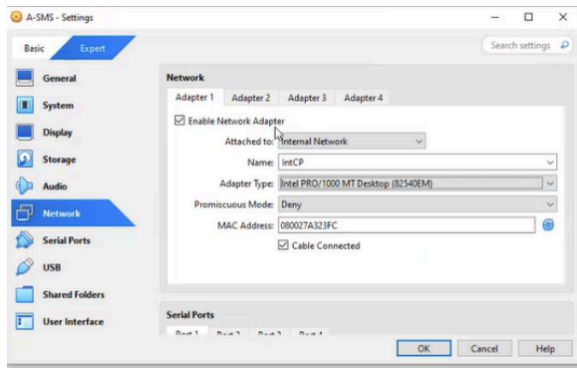
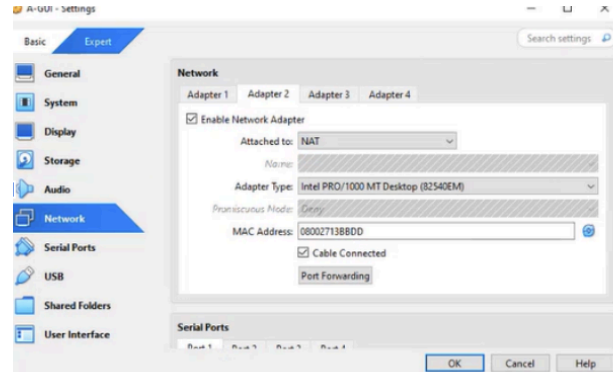
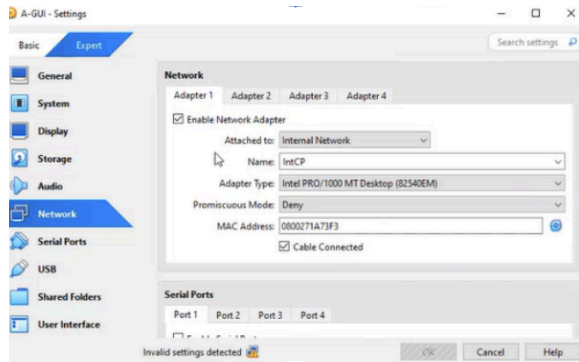
GAIA Appliances Overview

This security set up runs on the Check Point GAIA operating system which is a secure and hardened operating system which is the basis for all deployed security appliances. GAIA offers a common environment for gateways and management servers including powerful command-line and web-based management facilities. The implementation uses three relevant parts of GAIA, that all have a certain role. Check Point Security Gateway (A-GW) is the main enforcement point in the network perimeter. It looks at all the traffic (both entering the internal network and leaving the internal network) against a single-centre security policy. It provides a variety of protection mechanism like stateful firewall rules, application control, and here configured, URL Filtering, and threat prevention.

The central administration point is the Check Point Security Management Server (A-SMS). It stores the security policy database, deals with licenses and updates, collects logs, and communicates with all of the managed gateways. All configuration is done from this server. The GAIA OS provides the much-needed security, network, and system services that enable these appliances to run reliably in an enterprise. This design includes a clear separation of duties between management (A-SMS), enforcing (A-GW) and administrating (A-GUI). This model provides improved security by separating out management traffic, scalability by enabling the management of one SMS to control many gateways, and a clear audit trail for any and all configuration and policy changes.

Installation and Configuration of A-GW, A-SMS, A-GUI

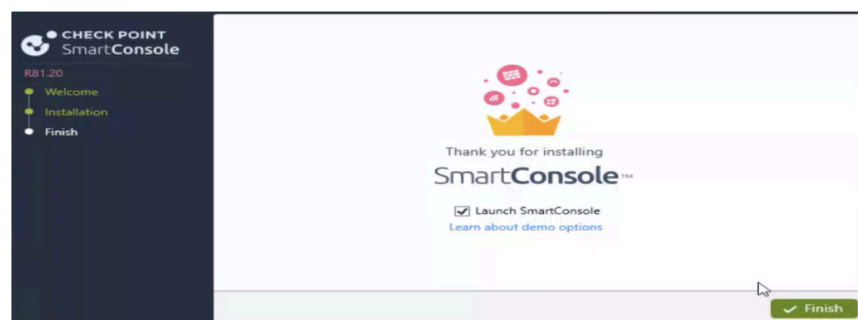
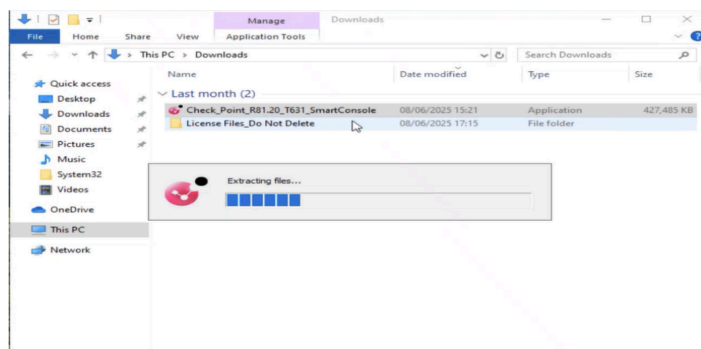
Configuring Network Settings



The Check Point lab is built on the network segmentation of Oracle VirtualBox. Its management plane is on a private internal switch with the name "IntCP." This switch is used to connect the important administrative elements: the management workstation (A-GUI), the Security Management Server (A-SMS), and Security Gateway (A-GW). This design creates a protected channel that is only used for management functions such as policy deployment and retrieval of logs that keeps this traffic entirely separate from user data flows. In order to make provision for any external communications needed (such as the fetch of software updates), both A-GUI and A-SMS have secondary network interfaces configured for NAT mode. This set up, along with allowing them a controlled outbound internet connection via the host system, ensures that the internal networks of the lab are isolated and secure.

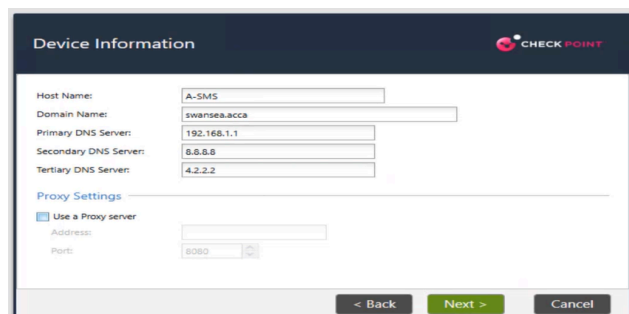
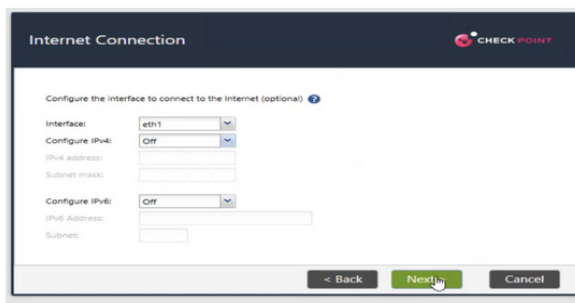
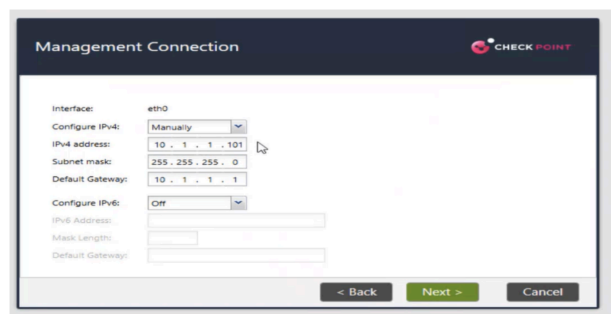
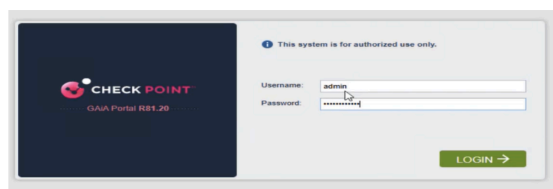
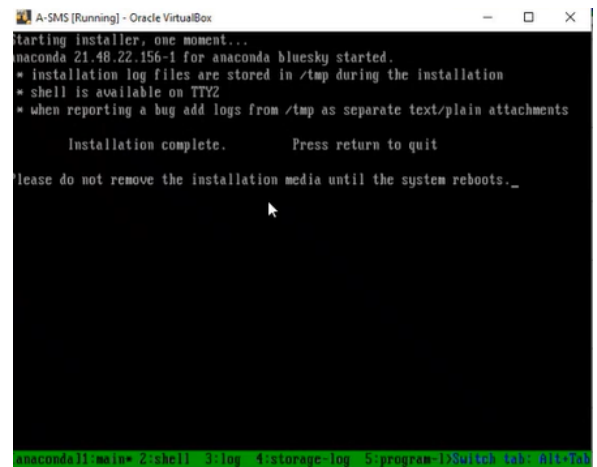
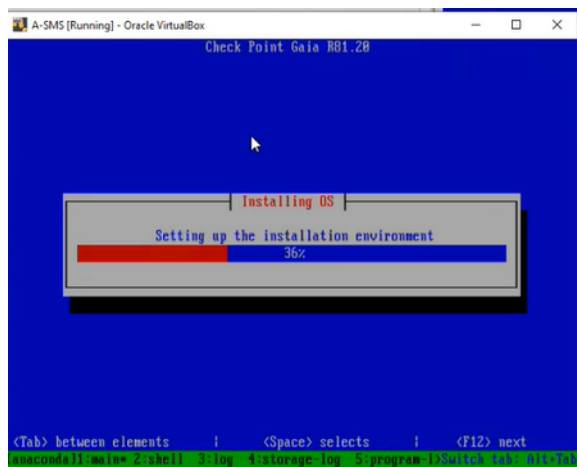
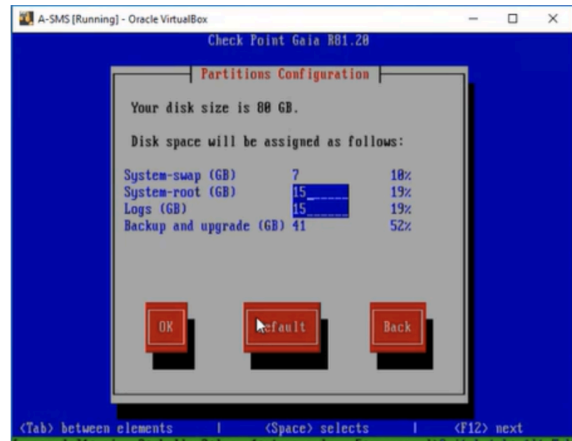
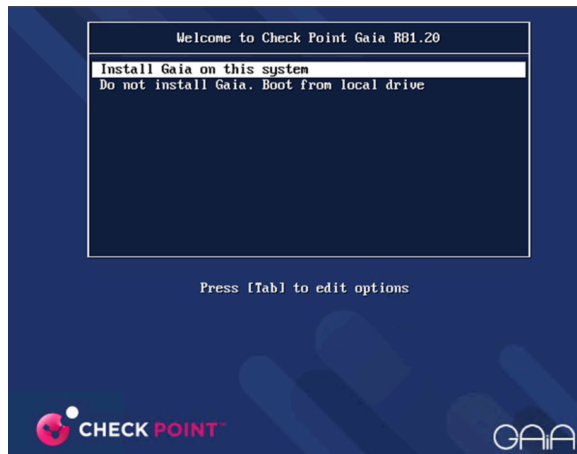
The Security Gateway (A-GW) is the central control point that enforces the security, with a multi-interface configuration, which is a good representation of a real corporate deployment. Apart from its main management connection to the "IntCP" network, the gateway uses three other and independent adapters. One adapter uses NAT to simulate the connection with the external internet connection. A second is attached to "IntSwa" internal network - the local area network for the Swansea head-quarters. The third is connected via the "ExtLCD" network, which is the wide area network connection to the remote London branch. This clear segregation over four different interfaces enables the gateway to apply and enforce specific security policies between the management zone, the corporate LAN, and the distant branch office, and the mock public internet.

Installation of SmartConsole on A-GUI



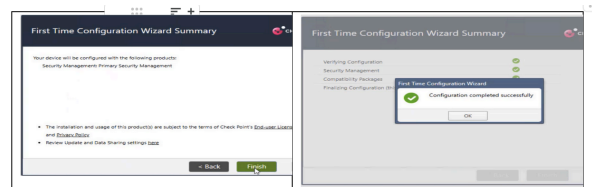
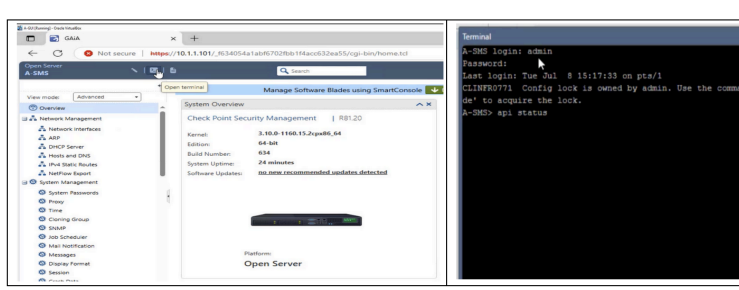
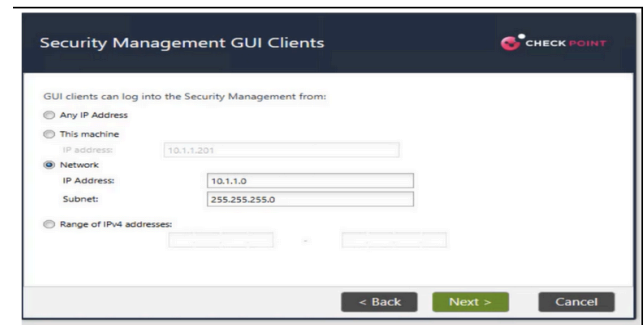
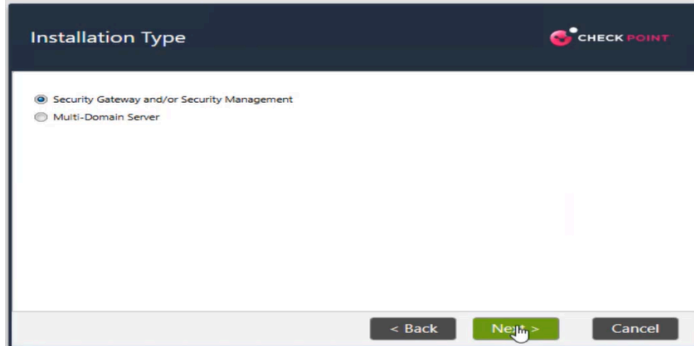
The following screenshots show the full installation sequence for installation of the Check Point SmartConsole client on the designated A-GUI management workstation. The procedure is triggered when the administrator runs the installation file that resides in the Downloads directory. The user interface then gives the initial "Extracting files..." progress indicator. Afterward, a status screen is displayed showing the installation progress at 15% and featured text promoting "Efficient Automated Operations." The last step in the visual workflow is a confirmation dialog, which is a sign that SmartConsole version R81.20 is installed successfully. This outcome results in a software tool that is ready for instant use in managing the security environment from a central console.

Installing the Primary Security Management Server (A-SMS)



SMS Installation The installation of the Check Point Security Management Server (A-SMS) begins by booting the Gaia R81.20 OS from its installation media. The 80 GB disk for the system is automatically partitioned with the default partitioning, which includes areas to store the root system, logs, swap space, and areas for eventual updates. The OS files are then copied to these partitions. A completion message is displayed, and a system reboot is then required to complete the installation and get into the new Gaia environment.

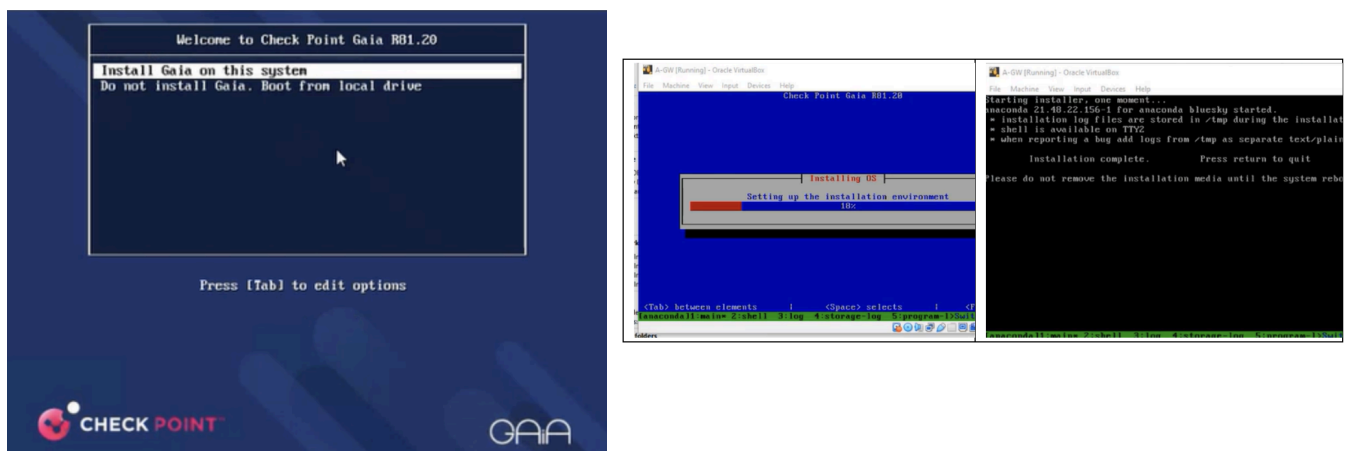
The administrator after rebooting uses the Gaia Portal through a web browser on the A-GUI client to run the First Time Configuration Wizard. One of the main tasks to be completed in this wizard is to manually configure the primary management interface (eth0) with the static IP address of 10.1.1.101, a subnet mask of 255.255.255.0, and a default gateway of 10.1.1.1. This integrates the server in the lab's dedicated management network. Configuration of secondary internet facing interface (eth1) is delayed. This basic network configuration allows the server to talk in the management segment, and also prepares the server for future setup.



The First Time Configuration Wizard proceeds with configuring the basic identity and role of the Security Management Server. The appliance gets the hostname "A-SMS", being joined to the domain "swansea.acca". DNS configurations have been made to use (by default) the internal Domain Controller at 192.168.1.1 (for internal name resolution), and to use (as a backup) external DNS servers for Internet access. The installation type is selected "Security Gateway and/or Security Management", which is suitable for a normal corporate lab (this does not choose the more complex Multi-Domain Server installation).

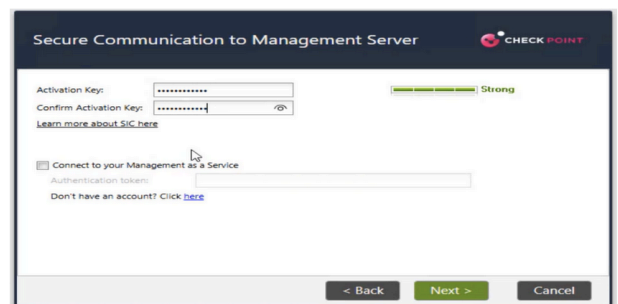
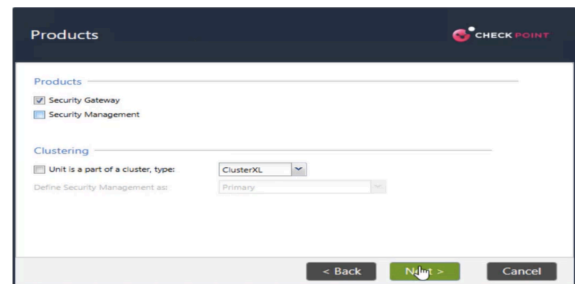
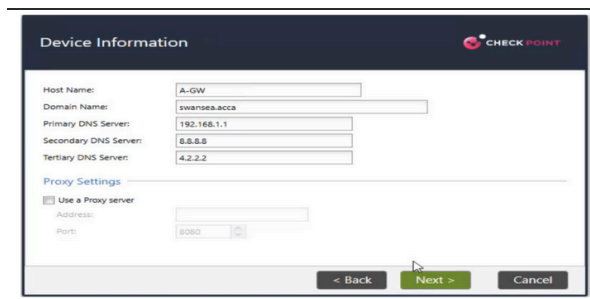
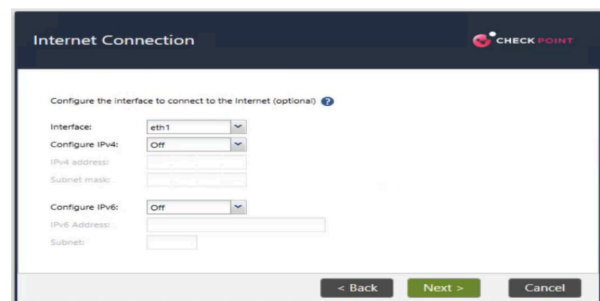
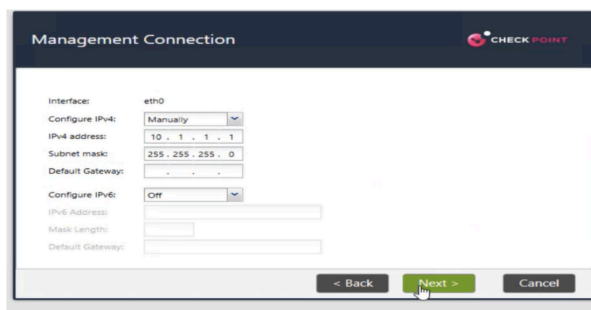
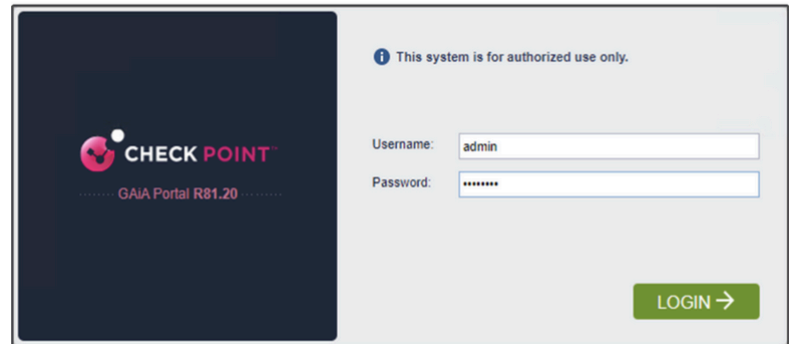
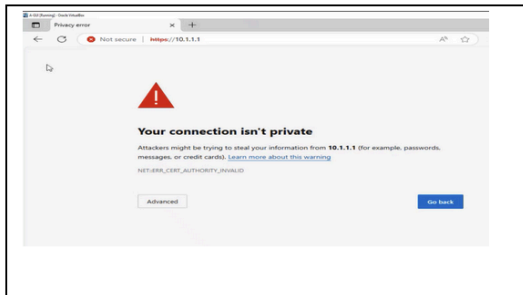
Next administrative access is locked down by specifying that only client IPs that are from the 10.1.1.0/24 management network are allowed to connect. This assures that management tools such as SmartConsole can only be opened from authorized workstations such as the A-GUI. The wizard concludes with a summary page that confirms the successful set up as a "Primary Security Management" server. Final verification is displayed in the Gaia Web UI System Overview confirming the R81.20 appliance is active and a terminal command is executed to verify that the critical API server is active.

Installation of the Check Point Gateway (A-GW)



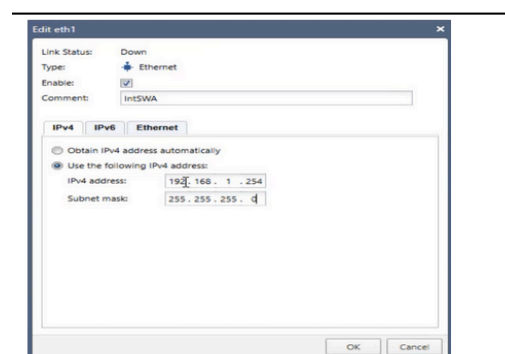
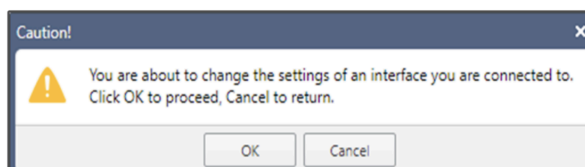
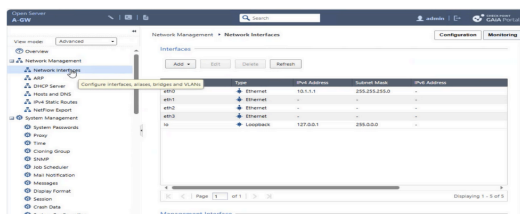
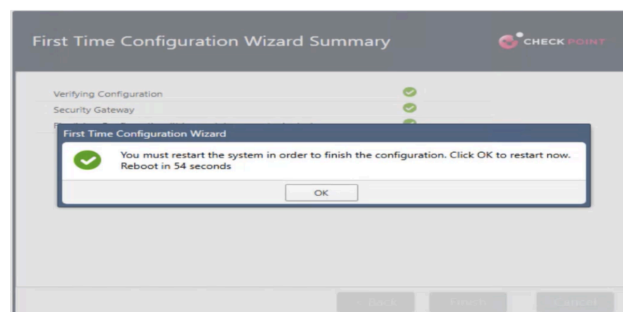
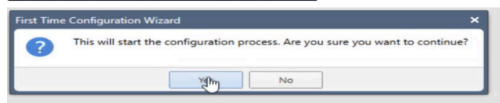
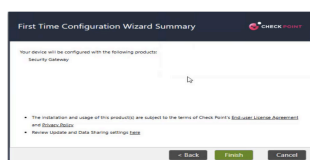
The installation of the Security Gateway (A-GW) starts with booting the virtual machine from the Check Point Gaia R81.20 ISO file. From the startup menu, the "Install Gaia on this system" option is chosen and the operating system deployment starts. This invokes an automated setup procedure, which is displayed by means of a progress bar on the screen. The process is completed with an "Installation complete" message and the subsequent press of the Enter key reboots the system to complete the gateway's initial setup.

.Running the First Time Wizard on the Security Gateway

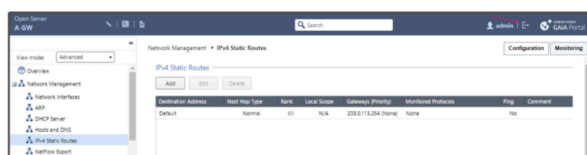
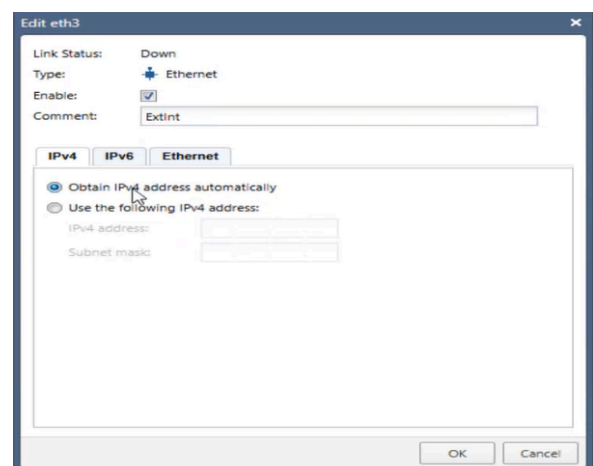
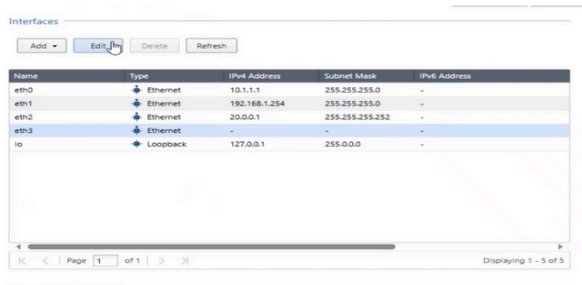
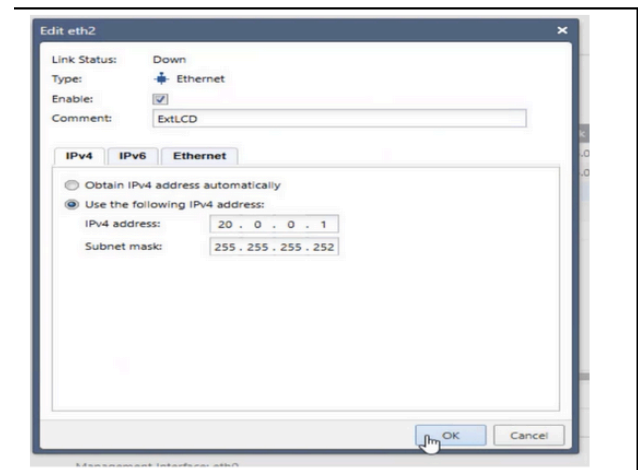
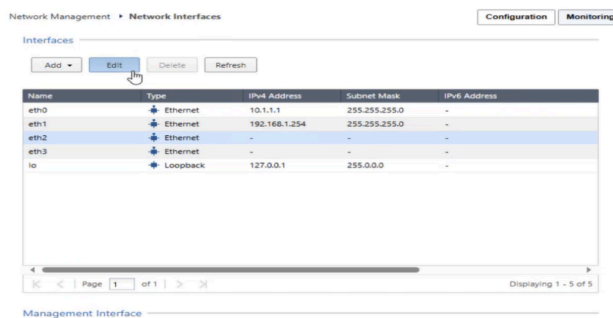


To configure the Security Gateway (A-GW) the administrator logs in to the Gaia web portal from the browser of the management client, bypassing security warnings about the browser's self-signed certificate. After invoking the First Time Configuration Wizard, the primary management interface (eth0) is verified with the IP address 10.1.1.1 and /24 subnet mask to be able to keep connected to the management network. Configuration for the external internet interface (eth1) is not done yet, both IPv4 and IPv6 disabled. Core identity settings are then applied, including hostname "A-GW" and Domain "swansea.acca" and DNS Servers - Prioritising Internal Domain Controller (192.168.1.1) and using Public DNS as a backup.

The setup proceeds further by specifying the purpose of the device: "Security Gateway" is specified as the role with the "Security Management" option left unchecked to make it a pure enforcement node. Clustering is still turned off, and a static IP address is assigned. The wizard concludes with the establishment of Secure Internal Communication (SIC) the administrator enters the activation key "Chkp!234" to create a trusted link enabling the Management Server to administer this gateway and deploy security policies to it.



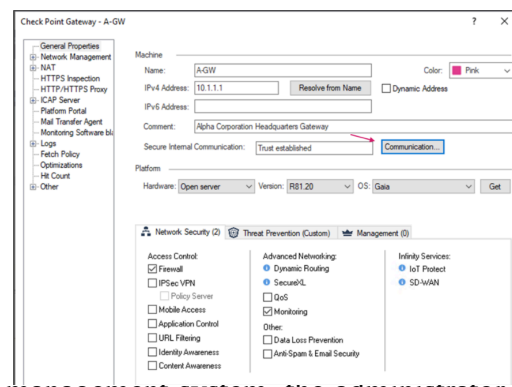
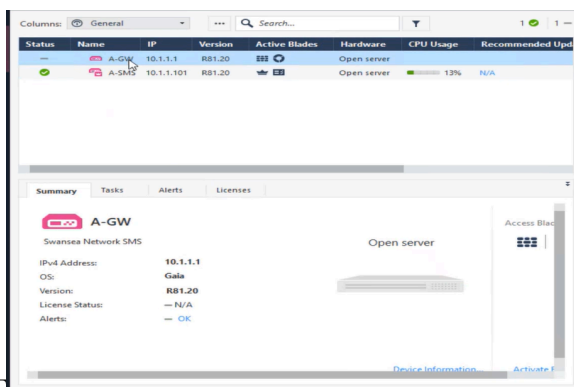
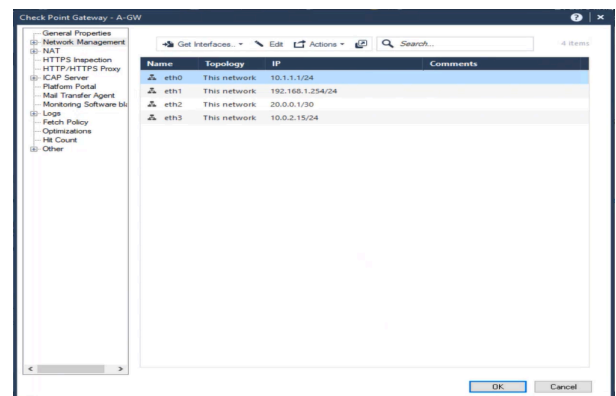
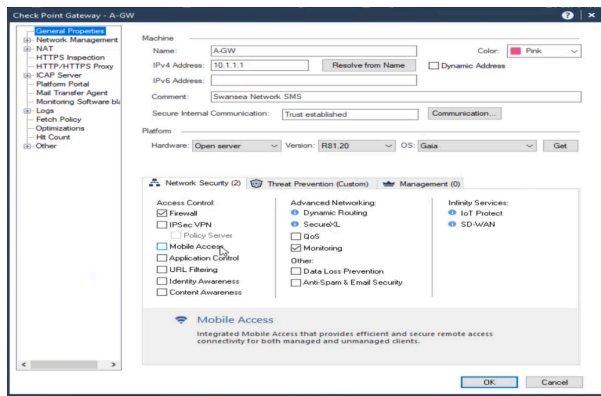
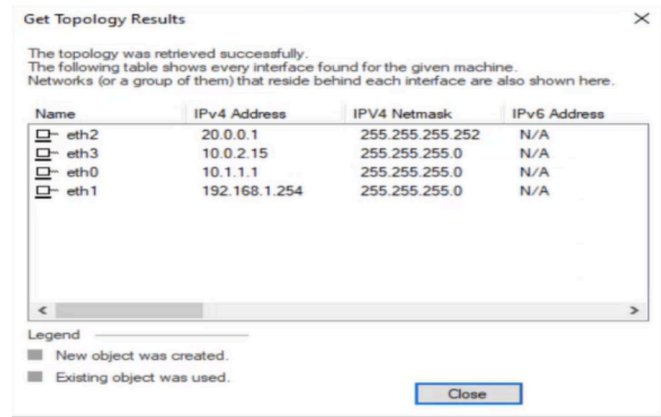
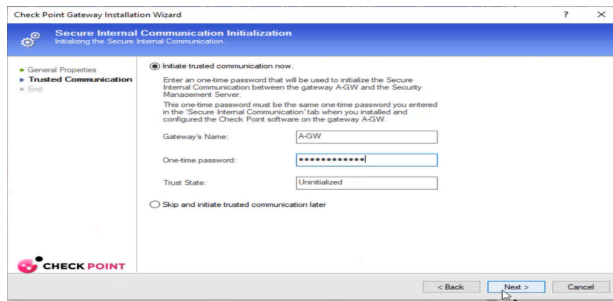
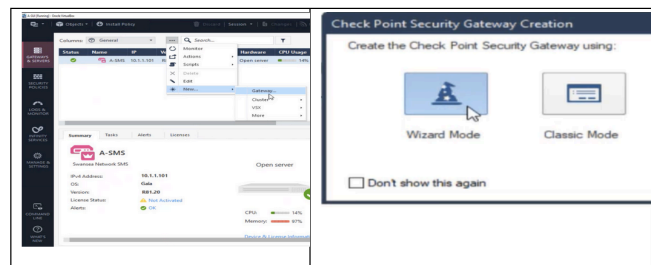
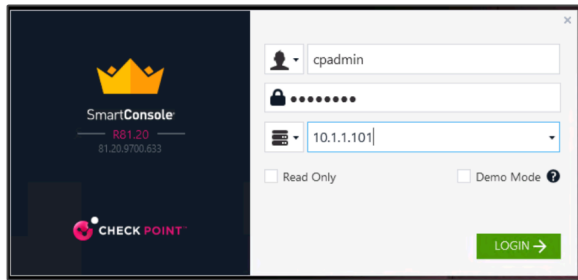
The setting up of the Security Gateway (A-GW) is performed by looking at the final summary in the First Time Configuration Wizard. Here, the administrator makes sure that the appliance is set up only as a "Security Gateway," and clicks "Finish" to save all settings. The system then needs a mandatory reboot in order to activate the new configuration. After rebooting the administrator logs back into the Gaia Portal to complete network setup. In the Network Interfaces menu the Management interface (eth0) is checked and confirmed to be active with the IP address 10.1.1.1. Next, the internal interface (eth1) is manually enabled and given the IP address 192.168.1.254. "IntSWA" has been added to know that it is connected to the internal Swansea network.



This configuration phase is used to complete the configuration of the other network interfaces in the A-GW. The administrator edits the properties for interface eth2, makes it enabled and adds

the comment "ExtLCD." A static IPv4 address of 20.0.0.1 with a /30 subnet mask (255.255.255.252) is specified and this is set to be the dedicated link for the simulated London WAN connection. Next interface eth3 is enabled and labelled "ExtInt." Its IPv4 parameters are set to retrieve an address automatically through DHCP with the port considered dynamic-and internet-facing. After making all the changes to the interface, the administrator logs out of the Gaia Portal and closes the browser, completing the network configuration of the gateway and completing the lab session.

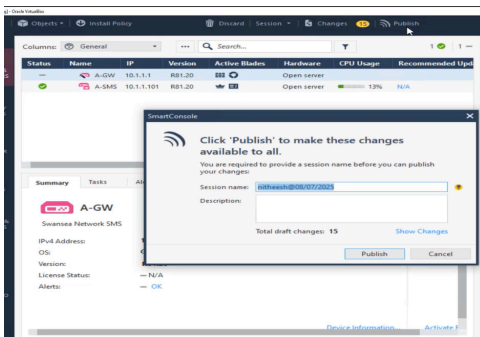
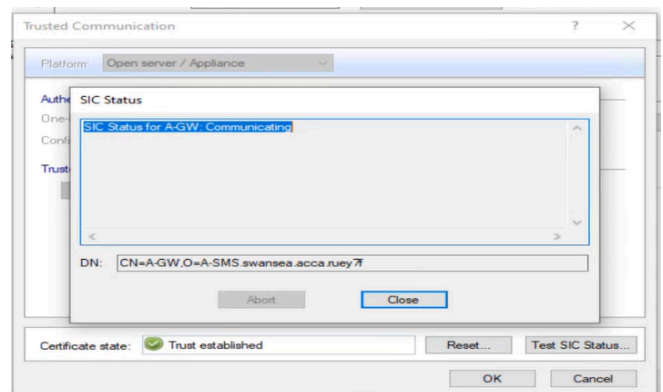
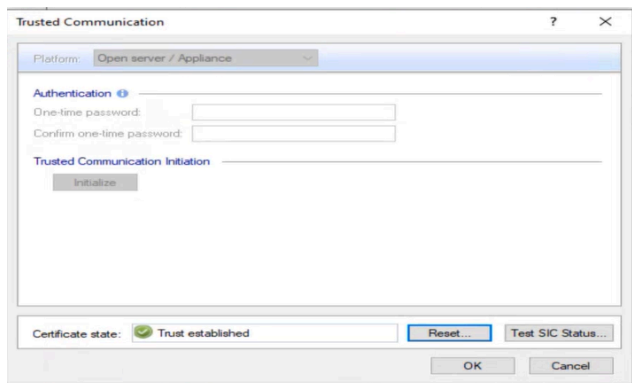
Establishing Secure Internal Communication



To establish the Secure Internal Communication (SIC) from the management system, the administrator needs to log into the SmartConsole application using the cpadmin username and the IP address of the

management server, 10.1.1.101. Inside the console, a new gateway object is created by starting up the guided Wizard Mode. The most important thing is establishing the Secure Internal Communication (SIC) trust. This is done by inputting the name of the gateway, A-GW, along with the same one-time password that was set on the gateway previously. Once SIC is successful, SmartConsole automatically retrieves and presents the full network configuration of the gateway with all interfaces and their IPs for review.

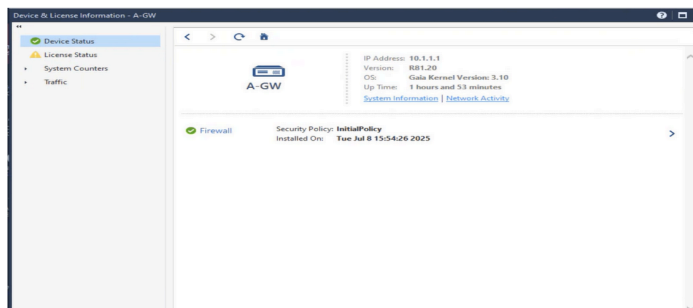
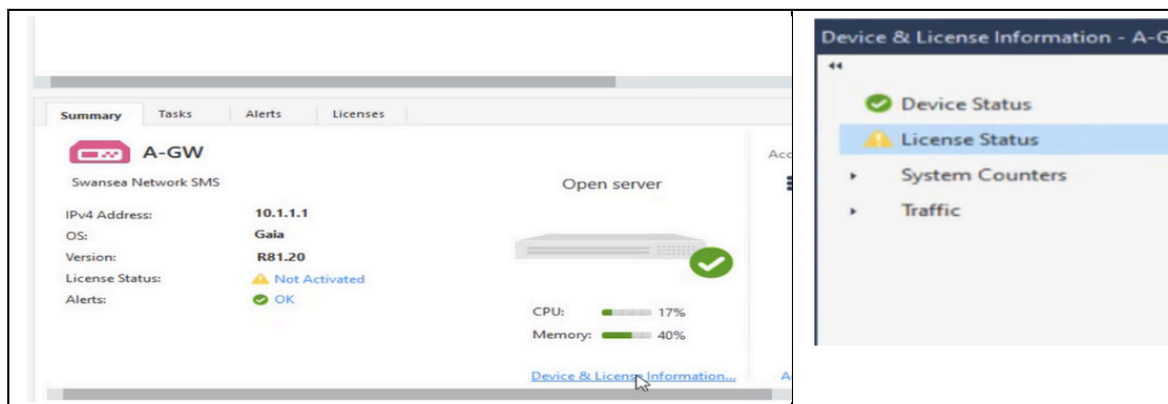
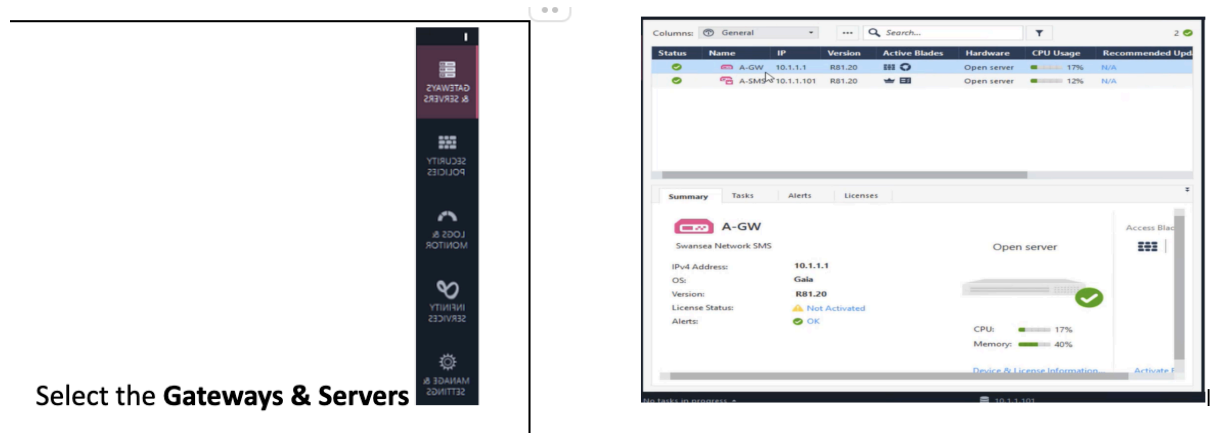
Then, the administrator makes edits to the new gateway's properties which actually allows the Mobile Access software blade to function and makes VPN possible. The list of interfaces (eth0, eth1 eth2 and eth3) is recapitulated in the console to ensure it properly. A-GW object is now in the main dashboard containing summary information. A final check of the gateway's properties checks the correct name and IP address and most importantly shows the status of the Secure Internal Communication as 'Trust established' which completes the integration process.



The screenshots illustrate the final steps to verify and save the Security Gateway configuration in SmartConsole, and focus on the trust of Secure Internal Communication (SIC). The administrator is able to check the connection by opening the "Trusted Communication" window, where the connection status is displayed as "Trust established," with a green checkmark. For more

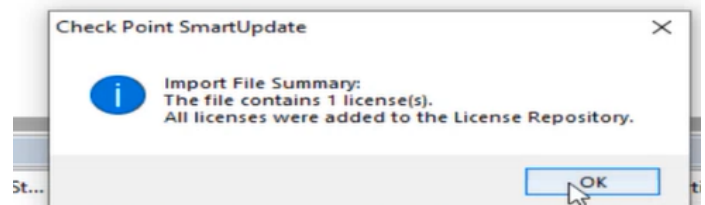
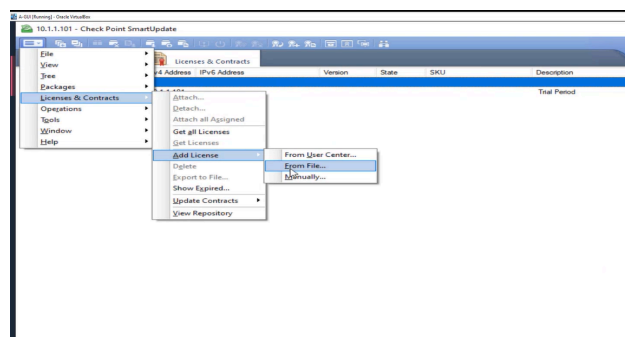
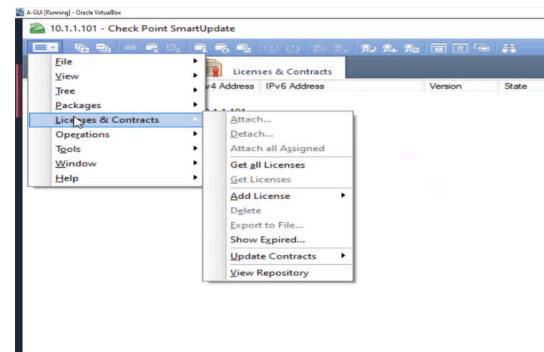
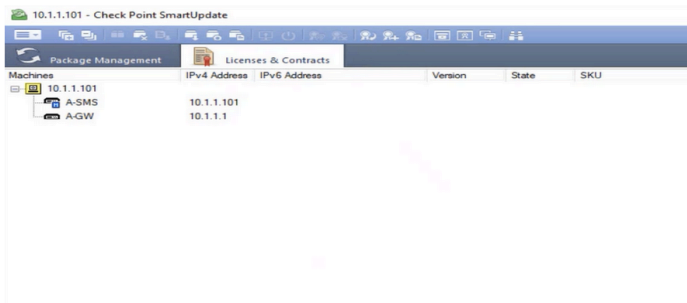
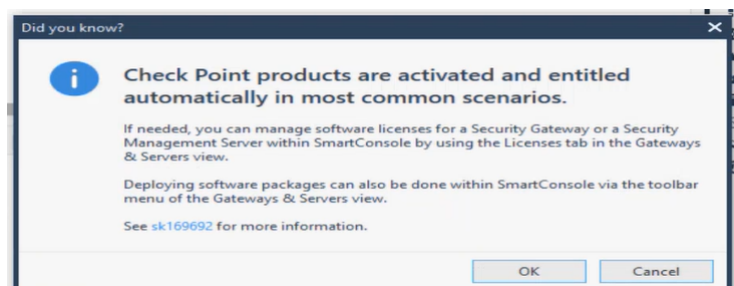
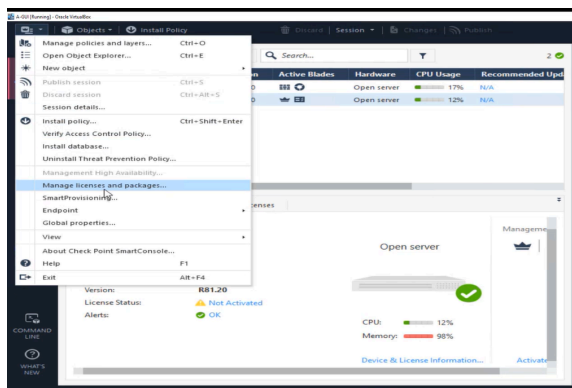
assurance, the administrator clicks on Test SIC Status that returns a successful message: SIC Status for A-GW: Communicating. This promises that the management server and gateway can communicate safely. To complete, the administrator closes the verification windows and clicks on the "Publish" button on the SmartConsole toolbar. With this action, the new gateway object and all the settings are saved to the database of the management server.

Managing Licence



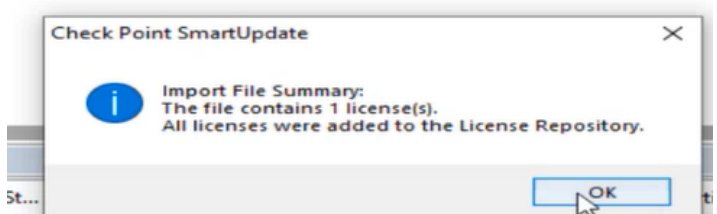
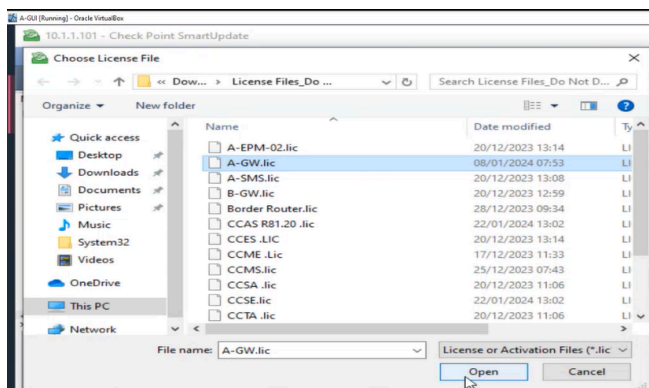
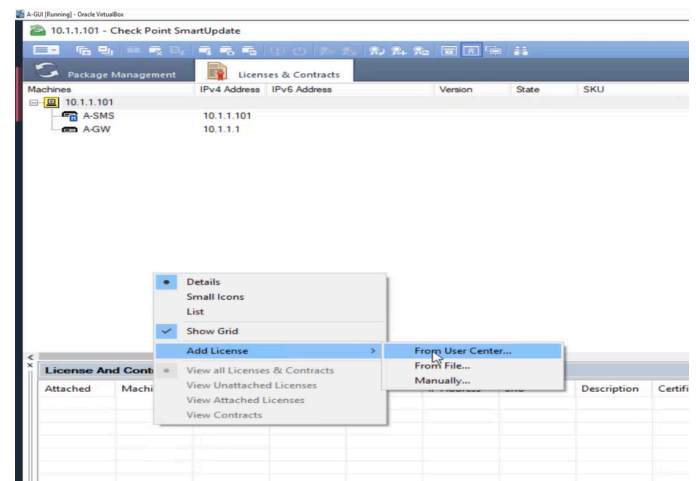
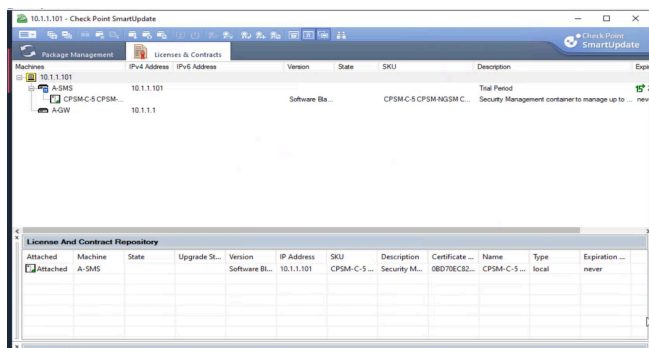
The in screenshots are documented the conclusive phase of the gateway configuration, which is centered around the validation of the Secure Internal Communication (SIC) trust state. Verification happens in the "Trusted Communication" interface where a successful "Trust established" status is displayed visually by a green checkmark icon. Another operational test is carried out using the "Test SIC Status" function; the positive outcome of this test is "SIC Status for A-GW: Communicating." This verifies that the encrypted control pathway between the management server and the gateway is completely working. The process is completed by dismissing the open windows and clicking the "Publish" action button that commits the new gateway object along with its configurations to the management repository.

Attaching a Licence Using SmartUpdate

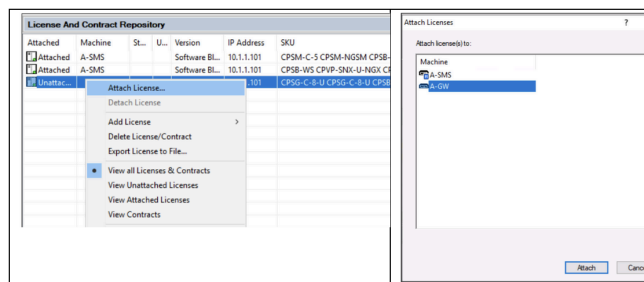
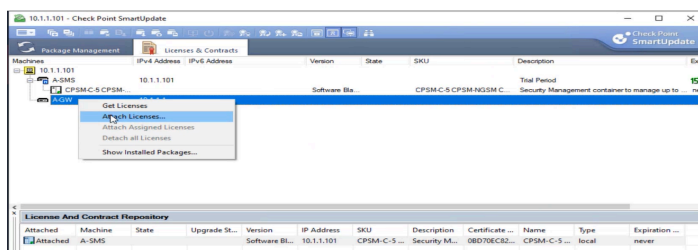


The license management process starts with the administrator accessing SmartConsole and traveling the menus to access the separate "Manage licenses and packages" tool. An initial informational message about automatic activation is acknowledged which reveals SmartUpdate interface. This window shows a hierarchical list of all the managed appliances, including the A-SMS and the A-GW. The administrator then goes to the "Licenses & Contracts" menu, and selects "View Repository", which brings up the main dashboard for all license entitlements.

Inside the License and Contract Repository a new license is imported by right mouse click in the main area as "Add License > From File". from the context menu. A file browser window opens and allows selection and uploading of the required license file from the administrator's workstation. On successful processing, a confirmation message box is displayed, which confirms that the content of the license has been read and that it has been registered in the repository. Dismissing this dialog by clicking "OK" finalizes the addition and the new license is available for deployment to the appropriate security device



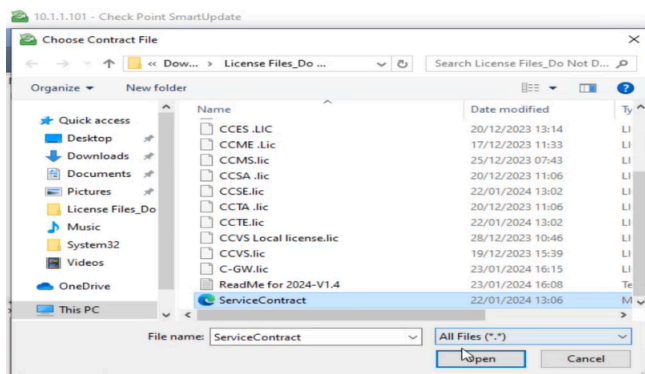
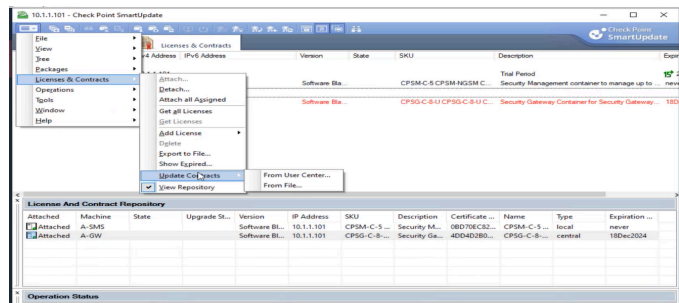
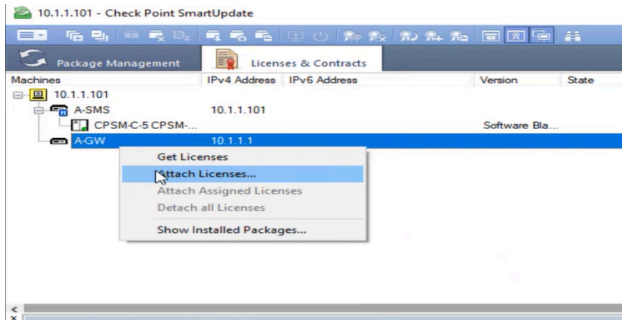
To perform the step of licensing, the administrator includes the required file by right-clicking in the License & Contracts repository panel and selecting "Add License > From File." A file browser opens up to choose the given license (for instance, A-GW.lic). Opening the file will cause a confirmation pop-up to open that verifies that the license was successfully added to the repo. The process is complete by checking the main SmartUpdate window where the new license entry should now be on the list of repositories with the status of "Attached". This verifies that the license is correctly associated with the device for which it is intended (as the A-SMS) and is valid, usually indicated with a permanent "never" expiration date



License And Contract Repository										
Attached	Machine	St...	U...	Version	IP Address	SKU	Description	Certificate	Name	Type
Attached	A-SMS			Software BL...	10.1.1.101	CP5M-C-5	CP5M-NGSM CP5B-WK...		Security Management container to manage up to	local
Attached	A-SMS			Software BL...	10.1.1.101	CP5B-W5	CPVP-SNX-U-NGX CP5B-S...		Web Security blade. SSL Network Extender for un	
Attached	A-GW			Software BL...	10.1.1.101	CP5G-C-8-U	CP5G-C-8-U CP5B-FW ...		Security Gateway Container for Security Gateway	

The Check Point SmartUpdate tool provides central management of licenses under the "Licenses & Contracts" tab. This view shows all the devices in the network such as the A-SMS management server and A-GW gateway in a tree format. In order to assign a license, an administrator can either pick a device (such as the A-GW) and select "Attach Licenses..." from the right-click menu, or (select available license in License And Contract Repository Pane and attach to desired device through same dialog). Success is verified in the repository list as the license status is changed to "Attached" indicating that software entitlements for both the management server and the gateway are now correctly linked and active.

Update the Service Contracts.



The screenshots depict the basic process for dealing with licenses and contracts when using Check Point SmartUpdate. First, go to the "Licenses & Contracts" Tab and view the network list. Select the A-GW gateway, right click and select the menu "Attach Licenses..." to take the first steps to assign a license to it. The next step, to update service agreements, choose "Licenses & Contracts" and then "Update Contracts" from the top menu. You can then decide to download updates automatically from Check Point's User Center or from a file on your computer. If using a local file then a "Choose Contract File" will open. Browse to your license folder and select the appropriate contract file (i.e. "ServiceContract") and click "Open" to import it into SmartUpdate.

Generating a Licence Report

The screenshots illustrate the process of generating a license report in Check Point SmartConsole:

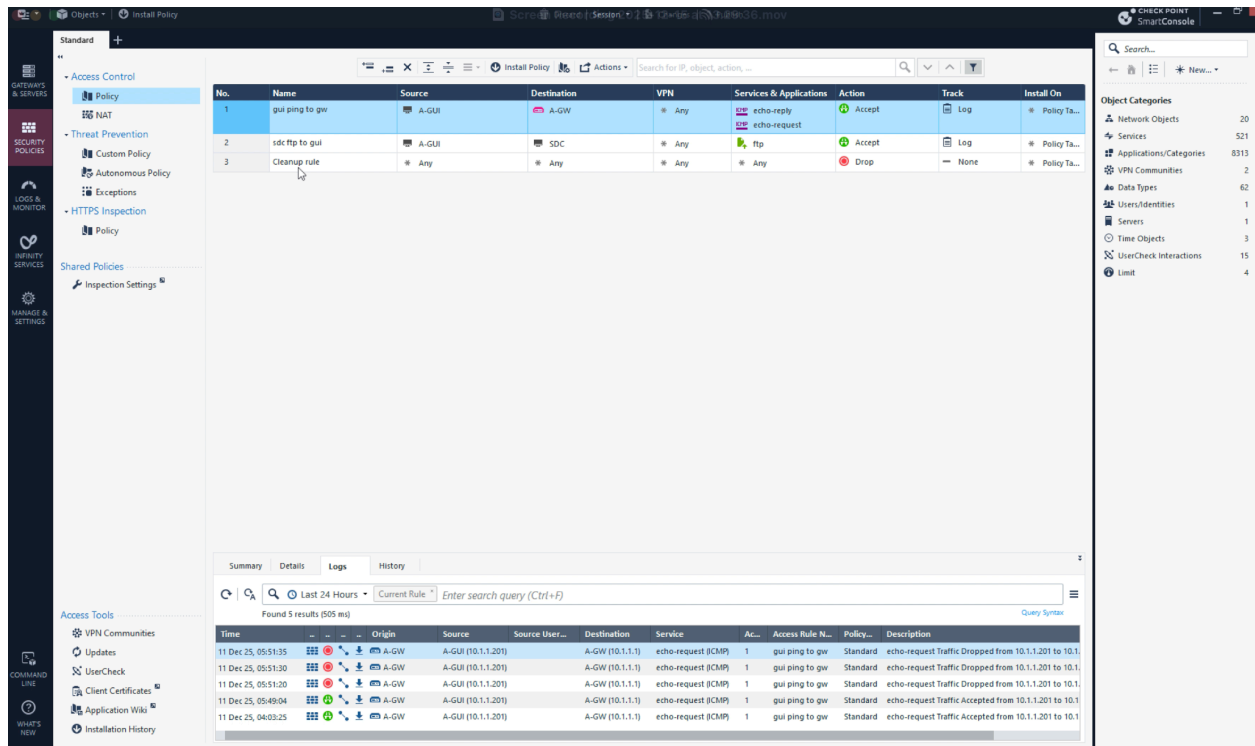
- Screenshot 1:** The 'Gateways & Servers' dashboard. The 'Columns' menu is open, and 'Licenses' is selected.
- Screenshot 2:** The 'Licenses' column is enabled. The table shows the following data:

Status	Version	License Status	CK	SKU	Account ID	Support Lev
OK	R81.20	N/A				
OK	R81.20	N/A				
- Screenshot 3:** The 'Actions' menu is open, and 'License Report...' is selected.
- Screenshot 4:** The 'License Inventory' report is generated. The 'Export to PDF' option is highlighted.
- Screenshot 5:** The 'Attach Licenses' dialog box is shown. The table lists the license to be attached:

Name	SKU	IP Address	Expiration ...
CPSG-C-8...	CPSG-C-8-U CPSG...	10.1.1.101	18Dec2024

In order to handle the licenses in Check Point SmartConsole, begin by customizing the "Gateways & Servers" dashboard. Enable the "Licenses" column to show important information such as the "CK" and "SKU" status fields that will indicate if a device such as the A-GW is unlicensed. For a full audit, create a "License Inventory" report of the "Actions" menu and take a PDF copy of this report for your records. To address the missing license, go to flow of the license (license attachment). In the last "Attach Licenses" dialog box, choose the appropriate license and click on the "Attach" button to attach it to the gateway.

Firewall Rules Configuration and Enterprise Security Policy Implementation

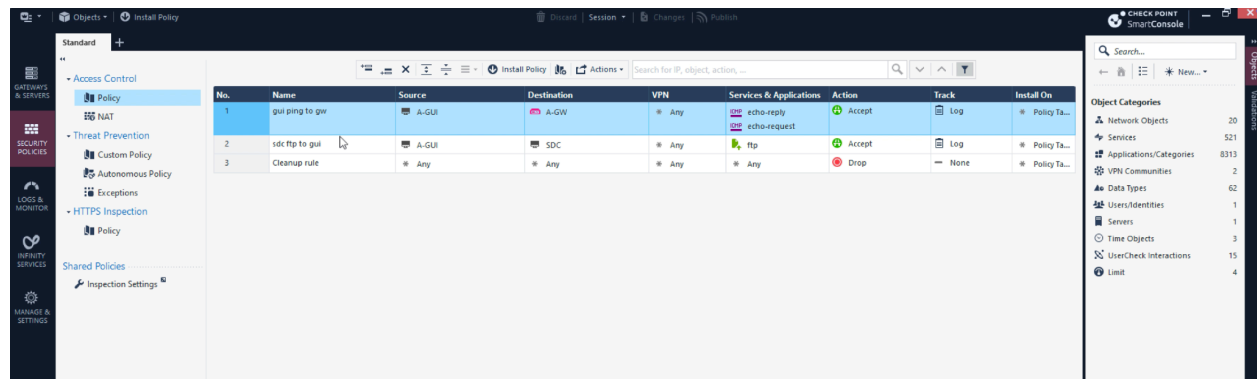


The screenshot is the Check Point SmartConsole, which is the main graphical interface for managing the security environment. This all-in-one dashboard integrates policy editing, objects management and real-time monitoring to make it easier to administer. The left side or sidebar provides quick access to some of the various sections, such as Gateways & Servers, Security Policies, Logs & Monitor. On the right the Object Categories panel is a searchable library of network objects, services and applications to make the rules consistent.

The central Access Control policy pane is where the traffic rules are defined. Rules are processed in the order of their occurrence. In this example there is explicit rules of Accept ICMP ("gui ping to gw") and FTP ("sdc ftp to gui") followed by a default Drop rule called "Cleanup." This is according to a "positive security model"--that is, only that traffic is permitted which matches a defined rule; everything else is blocked. source, destination, service, action or logging are finalized in each rule.

Policy configuration is a straightforward drag and drop operation. To create or edit a rule, you can either click New Rule or right-click in the rulebase, which opens the rulebase and a selector then moves the objects from the Object Categories panel to the either the Source, Destination, or the Services & Applications columns. Once changes are done, you have to click Install Policy in

the toolbar to compile and push the new rules to the security gateways which will make them enforced on live traffic.



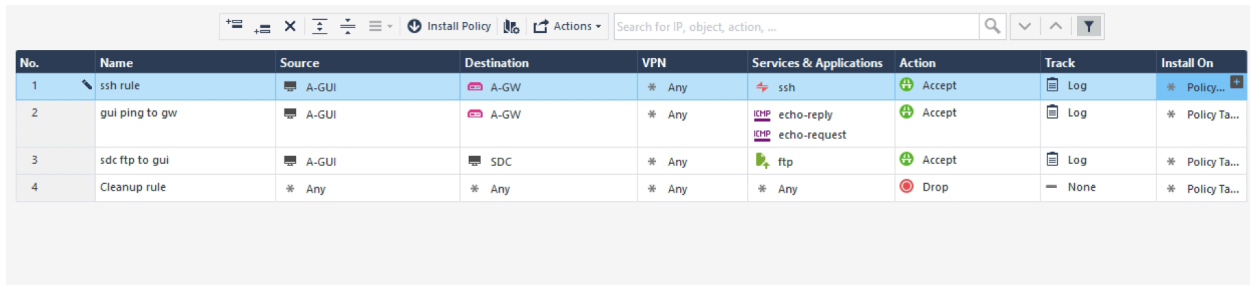
Configuring ICMP Policy

Ping is the basic network tool that makes use of the Internet Control Message Protocol (ICMP) to determine if a device is reachable and the delay of the connection. Unlike TCP or UDP which deal with application data, ICMP deals at a lower level to provide reports of error and for testing simple connectivity. A ping sends an "echo-request" packet and waits for an "echo-reply" giving vital information such as packet loss and latency, so it's an important first step in network troubleshooting.

The decision as to whether to permit or deny ping is a question of weighing security against operations. Blocking all ICMP can hide your network from simple scans but it also records useful diagnostics as well as cause technical problems. A very typical balanced approach is to only allow ping from trusted management networks to critical infrastructure and to block this from untrusted zones such as the public internet. This allows administrators visibility they need, while not subjecting the network to an excessive amount of risk.

In Check Point SmartConsole, this is achieved by the creation of an accurate rule. As you can see from this sample rule with the name "gui ping to gw," the administrator specifies the exact source (A-GUI) and the destination (A-GW). Instead of permitting everything, only the specific "echo-request" and "echo-reply" ICMP services are allowed per the security best practice of least privilege. The action is set to "Accept" and logging is enabled so that there is an audit trail of all pings allowed to monitor for normal, suspicious activity.

Configuring FTP Policy



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...

The File Transfer Protocol (FTP) is a standard method of transferring files through a network using a client server model. It works by using two distinct elements: a command channel over port 21 to send Jazz commands comprised of keepalive messages, list commands to view the Gantt chart, query command, move command, and query operation command, and a distinct data channel (commonly on port 20) to transfer the actual files. This enables users to log-in and control files on a remote system and is therefore a common tool across many internal networks.

However, standard FTP has a major flaw, which is that it transmits all the data, including login credentials and file contents as plain unencrypted text. This makes it easy for an attacker to intercept sensitive information. In a secure network, the routine blocking of FTP is considered a good practice and encrypted FTPs (SFTP) and FTPS should be used instead. If business needs dictate standard FTP, then its use has to be strictly controlled. Access should only be granted to certain, known internal machines and users to minimise risk.

Creating a secure FTP rule in Check Point SmartConsole involves accuracy when configuring the rule in the SmartConsole. As you can see in a sample of a rule called "sdc ftp to gui" you will need to specify exactly the Source ("A-GUI") and Destination ("SDC"). The "ftp" service object should be added to the rule, which enables the firewall to deal with both the command and data connections. Set the Action to "Accept" and Logging on. This logging is necessary, as it helps to provide a record of all the file transfers for security monitoring and auditing purposes.

Configuring SSH Policy

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 an encrypted command line remote access protocol, which replaces unverified tools such as Telnet. It works with TCP port 22 and with encrypted login credentials and all the session data (that cannot be intercepted). This provides administrators with the possibility to safely manage devices such as firewalls and servers on untrusted networks. Because of SSH high level administrative control thereof, there shouldn't be allowed in every location.

Best industry practice is to implement by only allowing SSH from trusted and secured management workstations and specific infrastructure devices. This reduces the likelihood of an SSH attack being used by an attacker to move laterally throughout the network. Strong authentication and detailed logging should also be enforced in order to be able to trace every administrative session. The recently added "ssh rule" (Rule 1) is aimed at making this secure, controlled access possible. It specifically permits access to SSH traffic between the "A-GUI" Management station and the "A-GW" gateway. By placing this rule at the top of the policy this management traffic is prioritized and guaranteed to be allowed. The rule has been set to Accept with Logging which will provide a full audit trail of all SSH access attempts, hence security monitoring.

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 ping test is used to verify that the network setup and the firewall rules are functioning properly, making it possible to communicate between the admin workstation and the gateway in both directions. The Command Prompt displays "A-GUI" (the workstation at 10.1.1.201) getting replies from the gateway at 10.1.1.1 with no packet loss and a constant 2ms response time. This proves that Rule 2 ("gui ping to gw") which specifically allows ICMP traffic, is working the way it is supposed to.

The network diagram helps in tracing the path, A-GUI is on the management network (10.1.1.0/24) and A-GUI's gateway is A-GW (10.1.1.1). From then on the traffic can be sent to other parts such as the main Domain Controller (S-DC) on the 192.168.1.0/24 network or the Child Domain Controller (L-CD) on 192.168.2.0/24 over the 20.0.0.0/30 WAN link. Passing this ping test is a basic step, but a step that needs to be taken - it can confirm the basic routing and firewall policies are right in place before testing advanced 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:
```

In the screenshot we can see successful ssh connection from the admin workstation to the gateway (10.1.1.1). Running the command `ssh admin@10.1.1.1` tests the new "ssh rule" in the firewall which is doing a fine job of allowing traffic on TCP port 22. The connection invokes a standard security prompt in which the user needs to accept the host key fingerprint of the gateway (it is unseen) using ED25519 encryption by typing "yes". This makes the gateway known by the workstation. After acceptance, the system displays the legal warning banner and then asks for a password. This entire process proves that the firewall policy is working and remote management access is properly configured and reachable

Enhanced Security Implementation Through Advanced Check Point Features

Application Control and URL Filtering provide a fundamental aspect of Next-Generation Firewalls (NGFWs) that are able to manage web applications and internet access in detail. They go beyond basic port blocking, to be able to identify and control specific applications and websites, which is huge to stopping modern day threats that hide in legitimate traffic. These tools aid in solving some common problems such as unauthorized use of software, lost production time, data compliance issues and accessing malicious sites.

Configuration Process:

To configure these, initially you will want to turn the Application Control and URL Filtering software blades on your gateway in SmartConsole and ensure that you have the support for it in your license. Then, go and edit your Access control policy layer, and enable the "Applications and URL Filtering" option.

Then you will be creating certain rules. A simple, low priority rule should always block dangerous categories of applications such as anonymizers, peer-to-peer file sharing programs, and unauthorized remote tools for all users ("Any" source) going to the "Internet." Set the action to "Drop" and set "UserCheck" on to notify the user he/she is violating policy. For controlling productivity, define rules based on Identity Awareness as a means of targeting specific user groups (e.g. GeneralStaff). These rules can be used to block categories such as "Social Networking" or "Streaming Media" with a "Drop" action and a custom UserCheck message which makes the policy unambiguous for employees.

Time-Based Access Control:

Time-based policies allow you to set time limits to limit the access. This decreases the risk of abuse and limits access beyond the needed hours and helps to manage the bandwidth.

The first step should be to create Time Objects (e.g. "BusinessHours" as 9 AM to 5 PM, Monday-Friday) in the Objects menu. In your Access Control policy, be sure to display the Time column. You can then create a rule allowing GeneralStaff group to do GeneralStaff can access the web browsing ("HTTP/HTTPS" service), but only during the "BusinessHours" time object. Right after this immediately follow a similar rule with no time limit and action of "Drop." This pair of rules makes sure that access is only granted for the specific time window, and all attempts during out of hours will be blocked and logged.