

Checkpoint
security
solution TG
Enterprise's

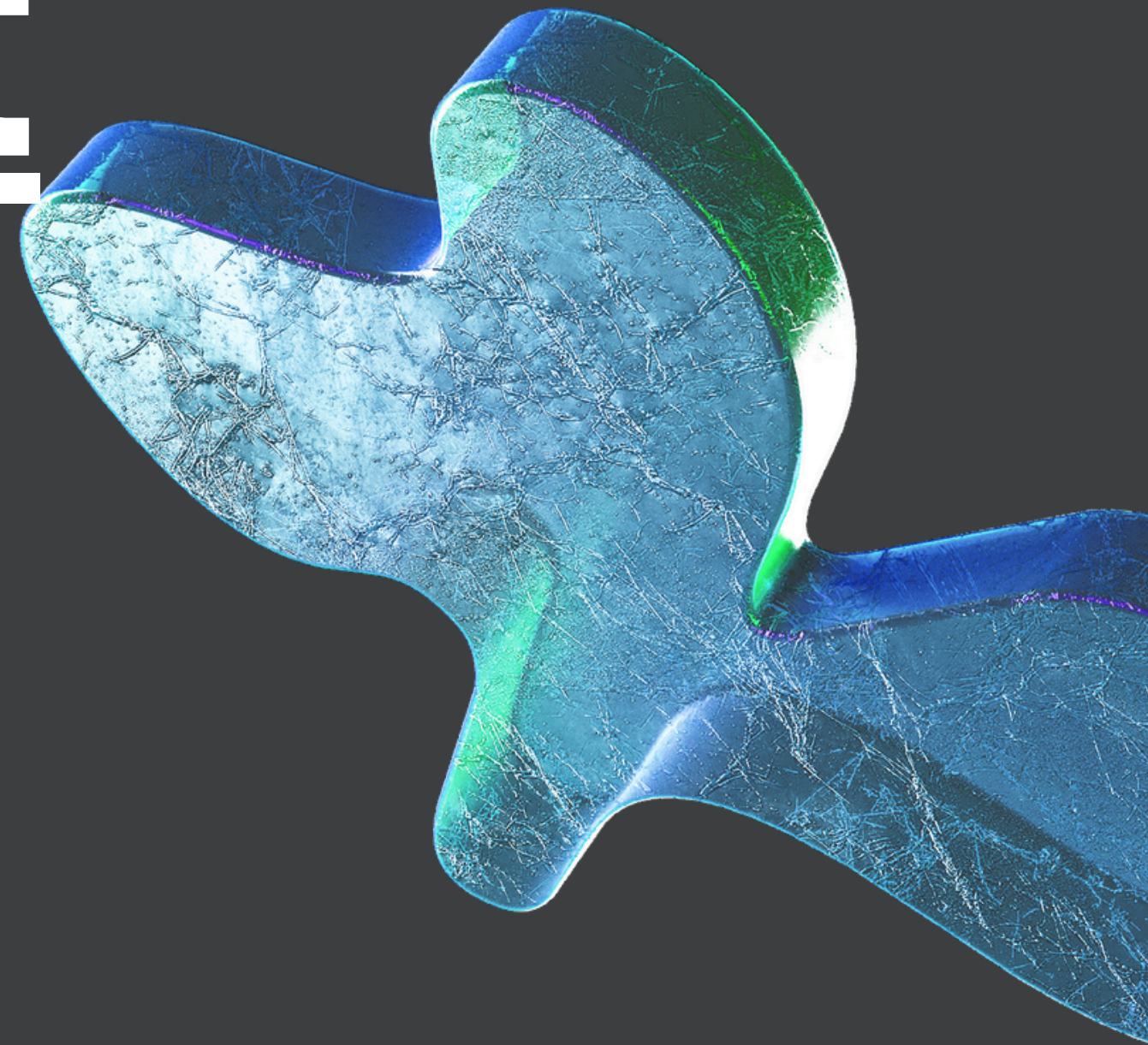
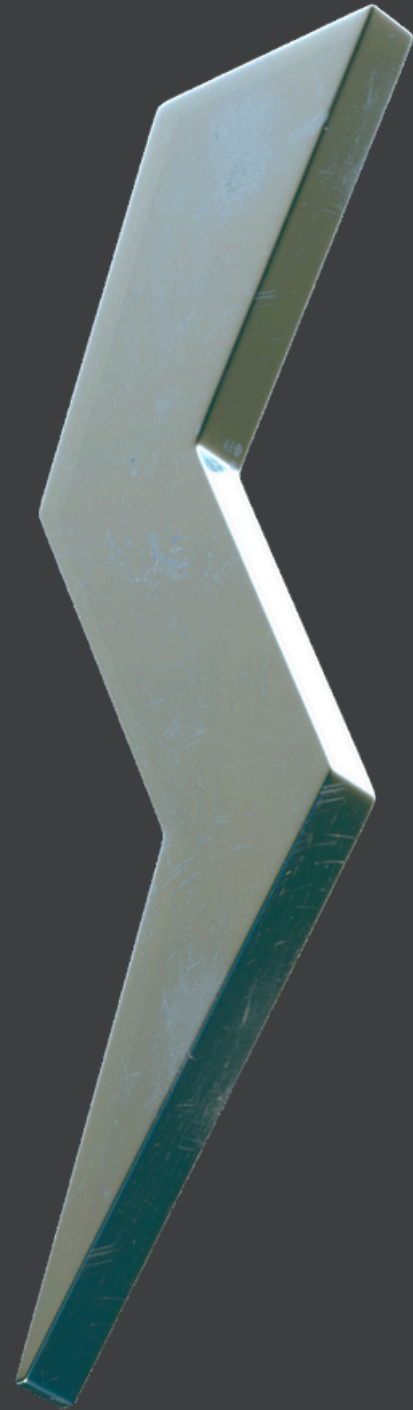


Table of Content



Explenation of the topology

Demonstration

Implementation of additional
security feature

Recommendations for future
improvements

Personal and Technical
Reflection

Conclusion

Objectives and outcomes

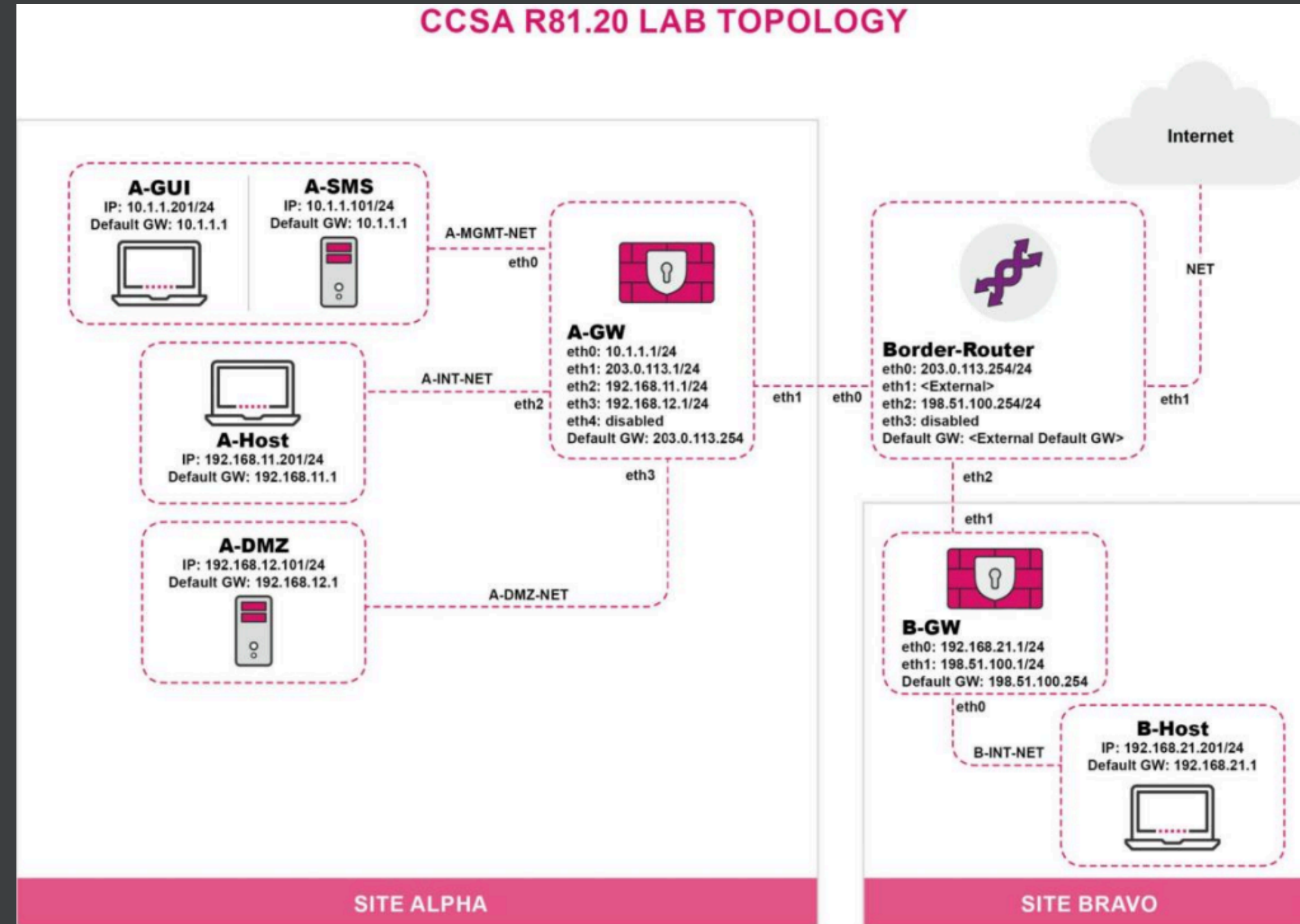
Problem : TG Enterprise's face several critical issues in its current security infrastructure.

Objective : Enhance the global security system of TG Enterprise's by implementing a checkpoint security solution.

Outcomes : Installation of basic security system with several issues that have been completed.

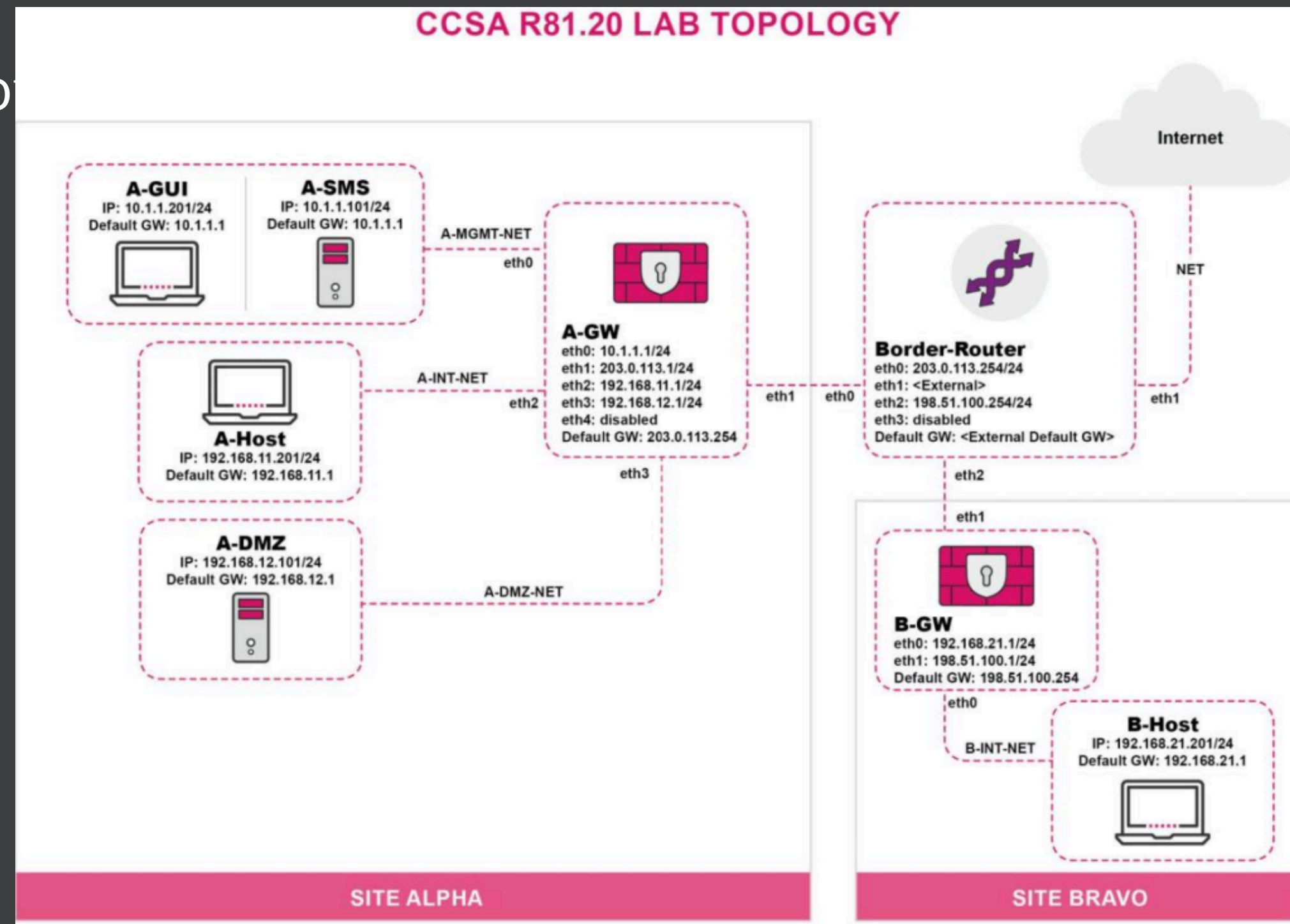
Existing topology

- A-GUI is the control center.
- A-SMS, B-GW, A-DMZ work on GAIA while A-GUI, A-HOST and B-HOST work on Windows.
- A-GW control the flow for the outside entry
- Single point of failure.
- Impossibility to connect B-GW to the Border router.



Context of TG Enterprise's

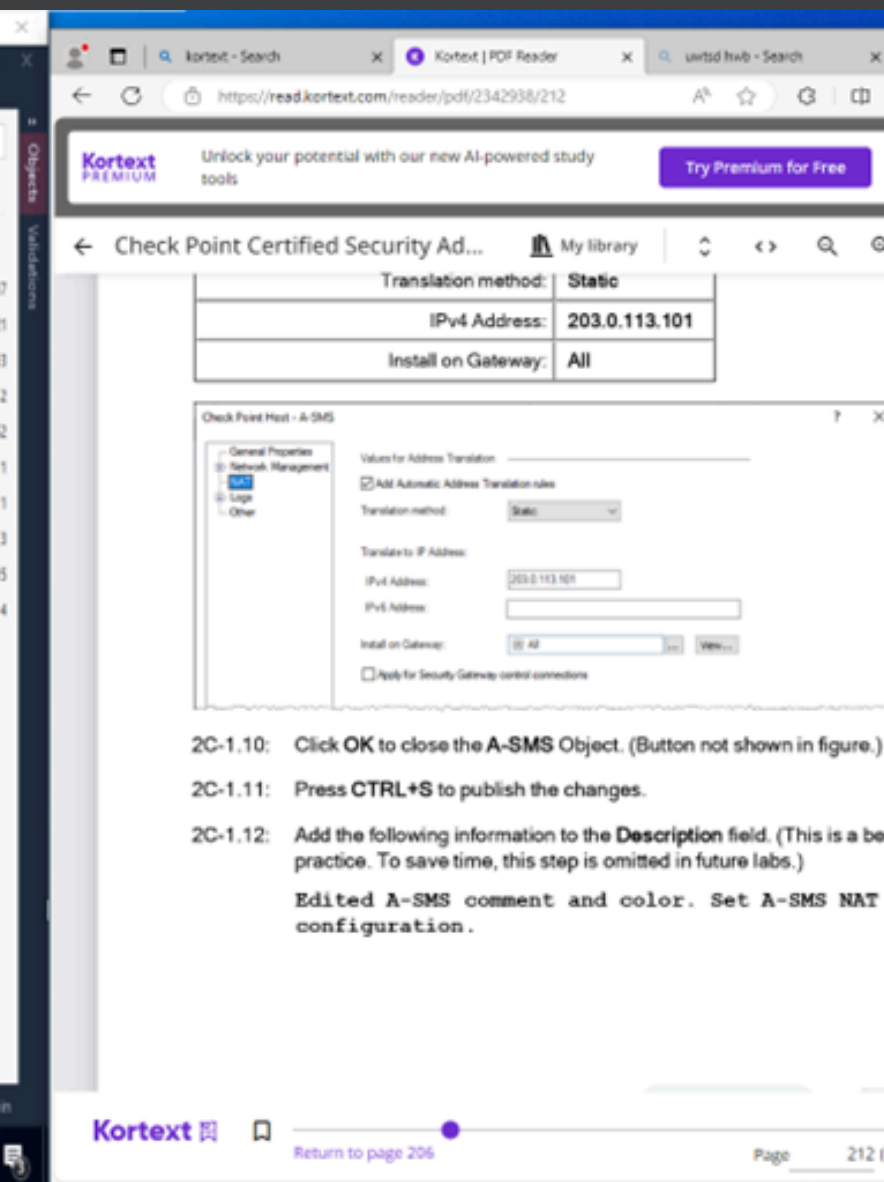
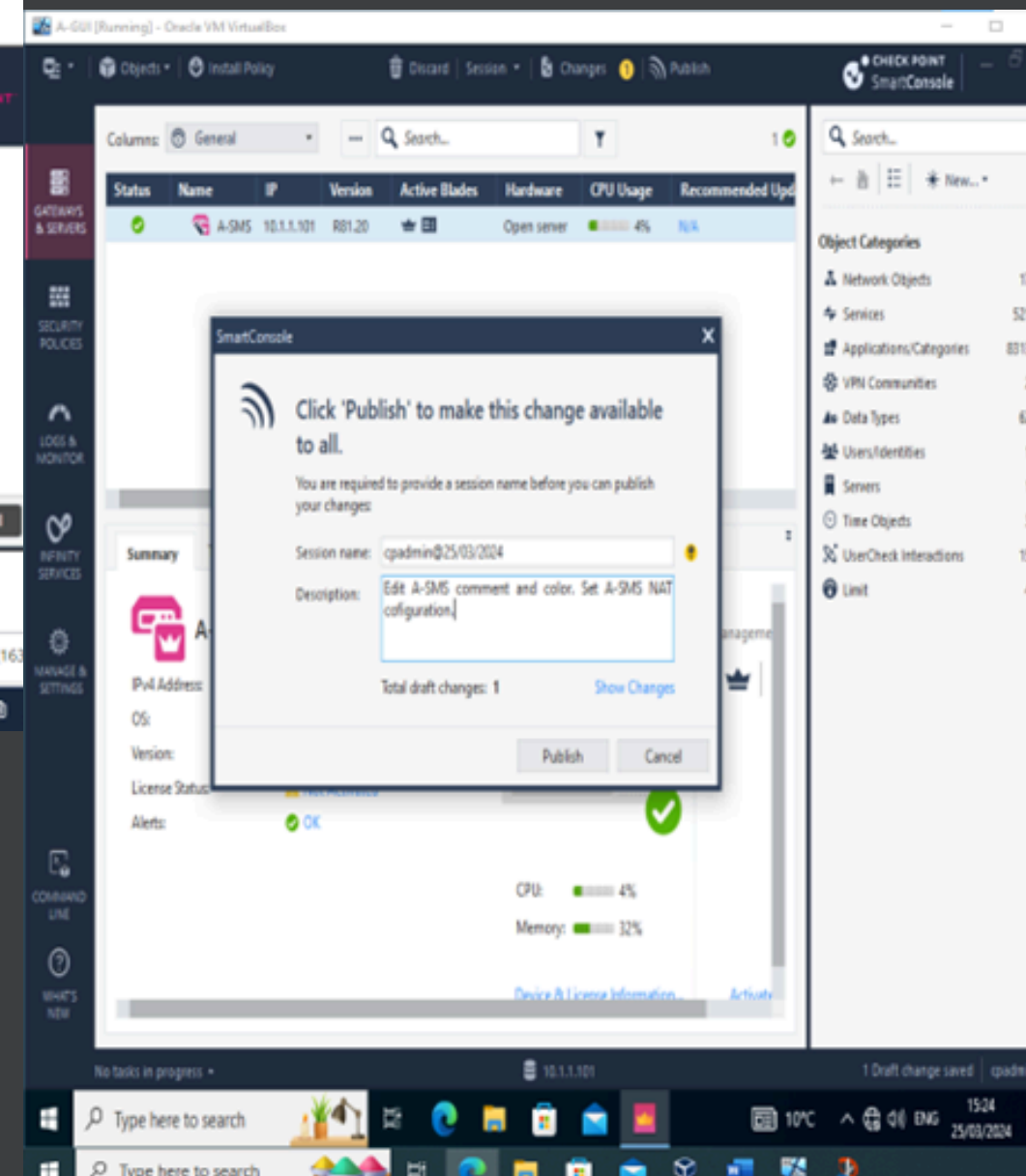
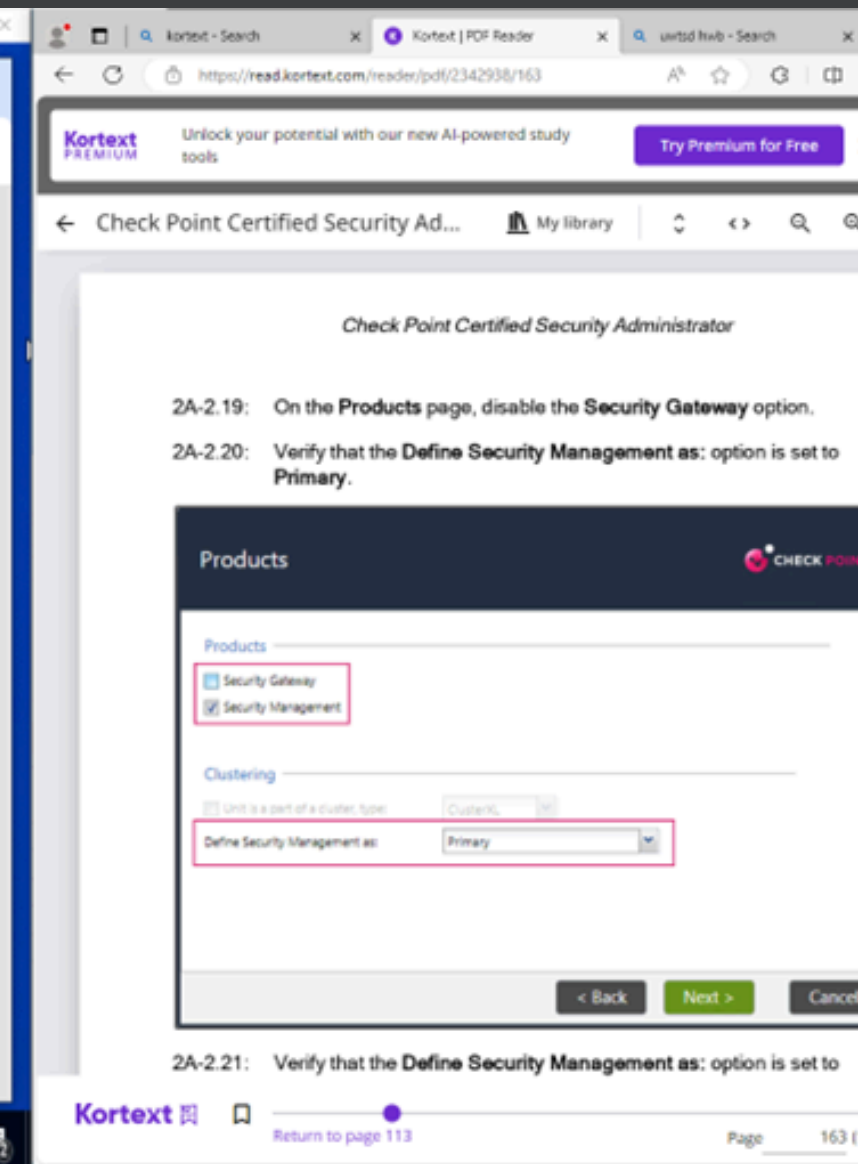
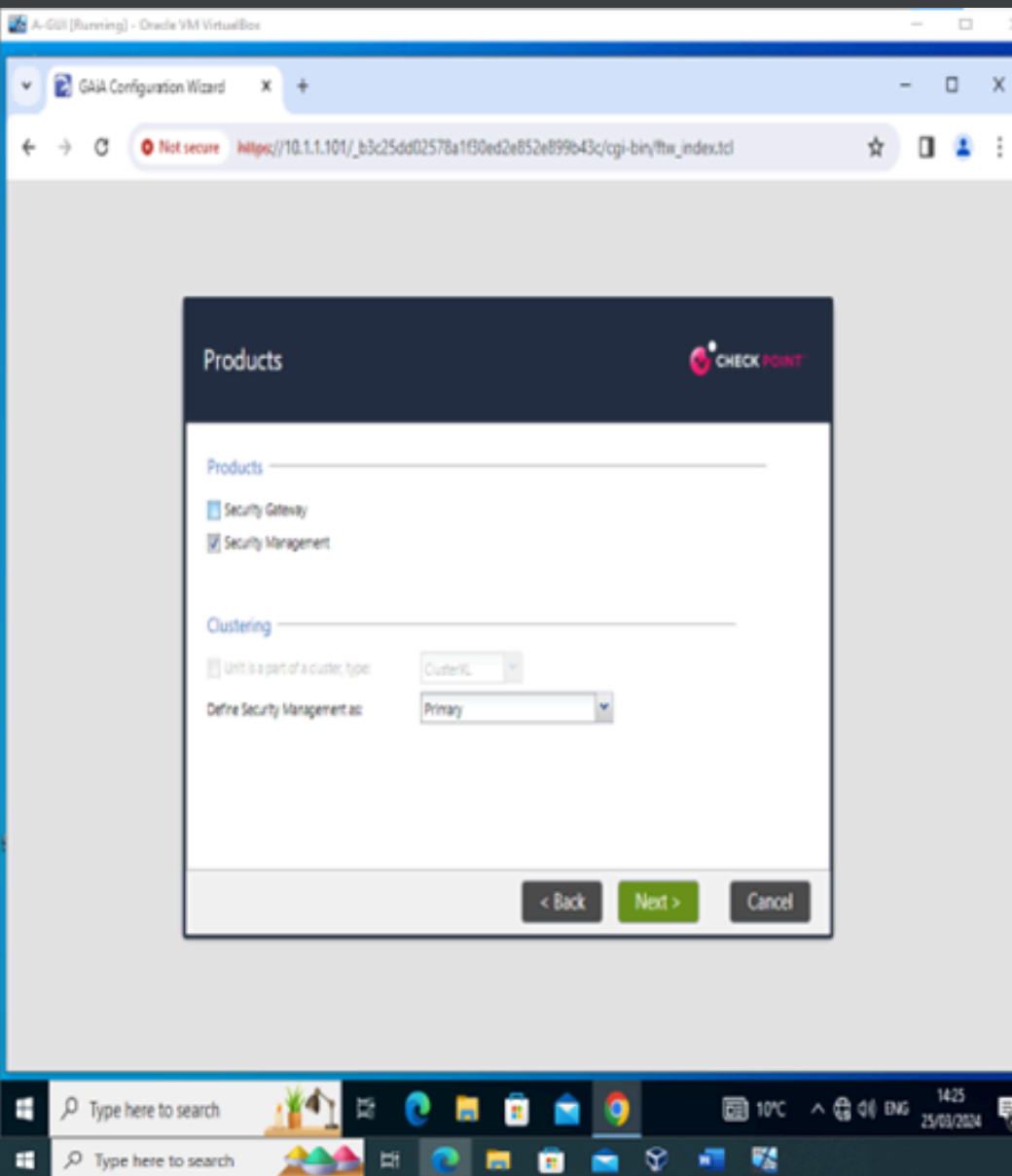
- Security audits and updates are irregular.
- Problem posed by IOT devices.
- There are SPOFs.
- Lack of control over application access.
- Inefficiencies result and errors in term of policy management.
- Costly and unnecessary features on the current licensing.
- Undefined roles and permission.
- Overlapping and conflicting policies.
- The IPS Rules are outdated.



Live demo

Lab : Gateway and server deployment

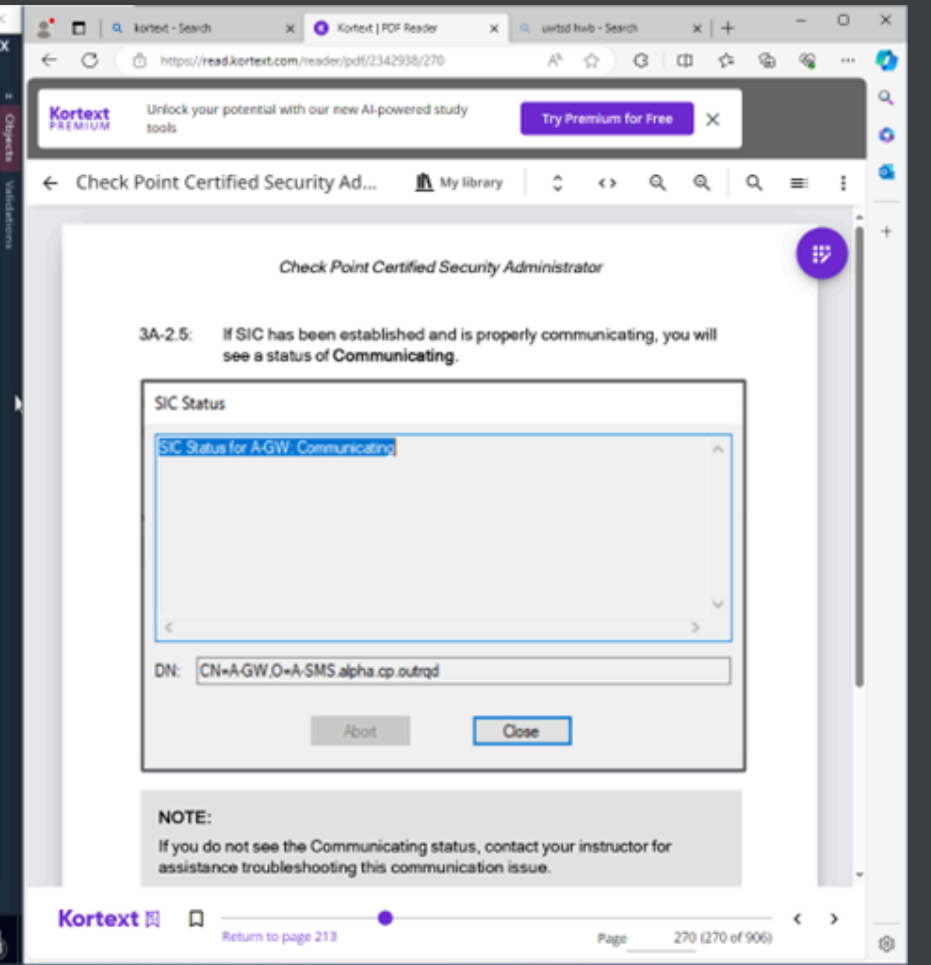
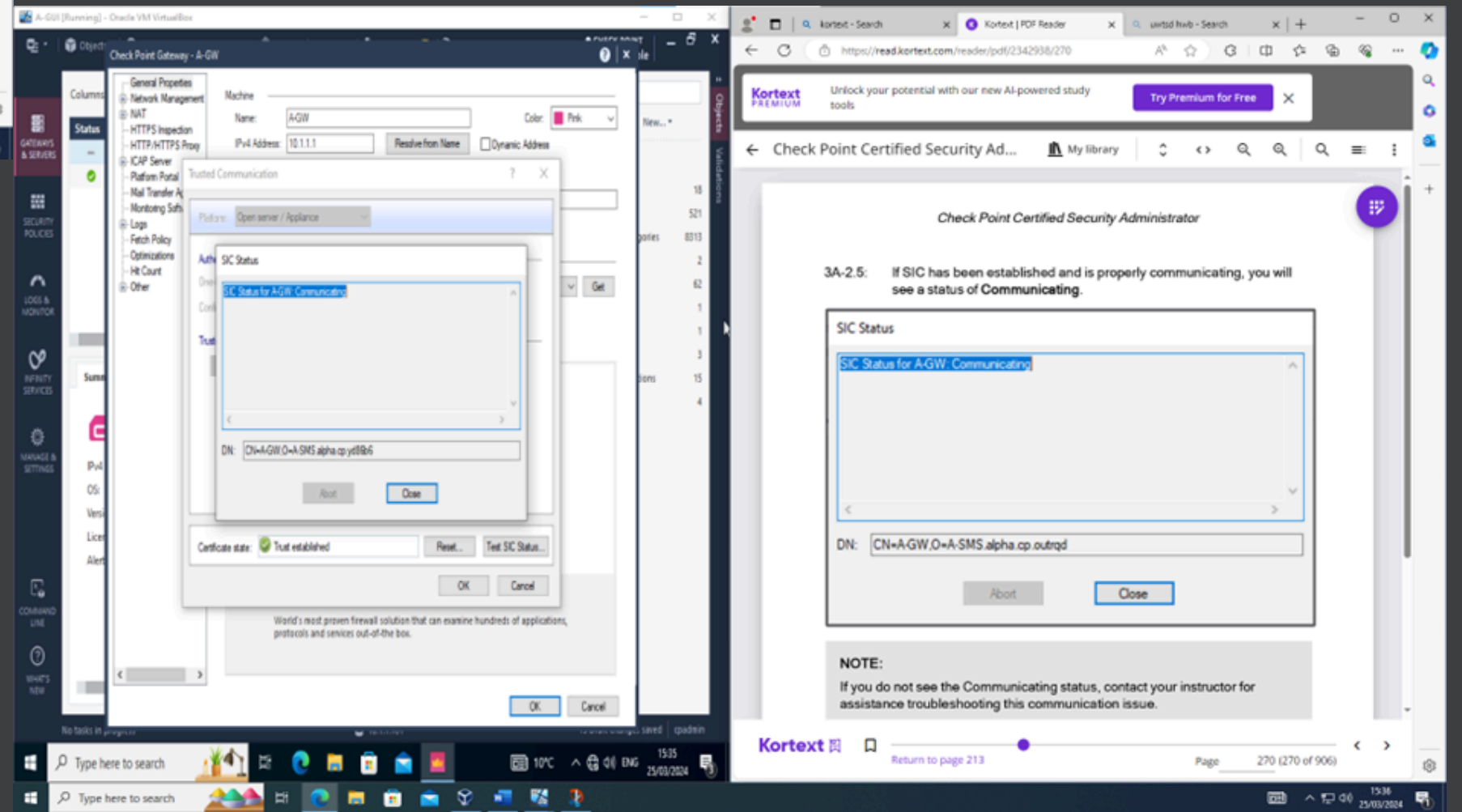
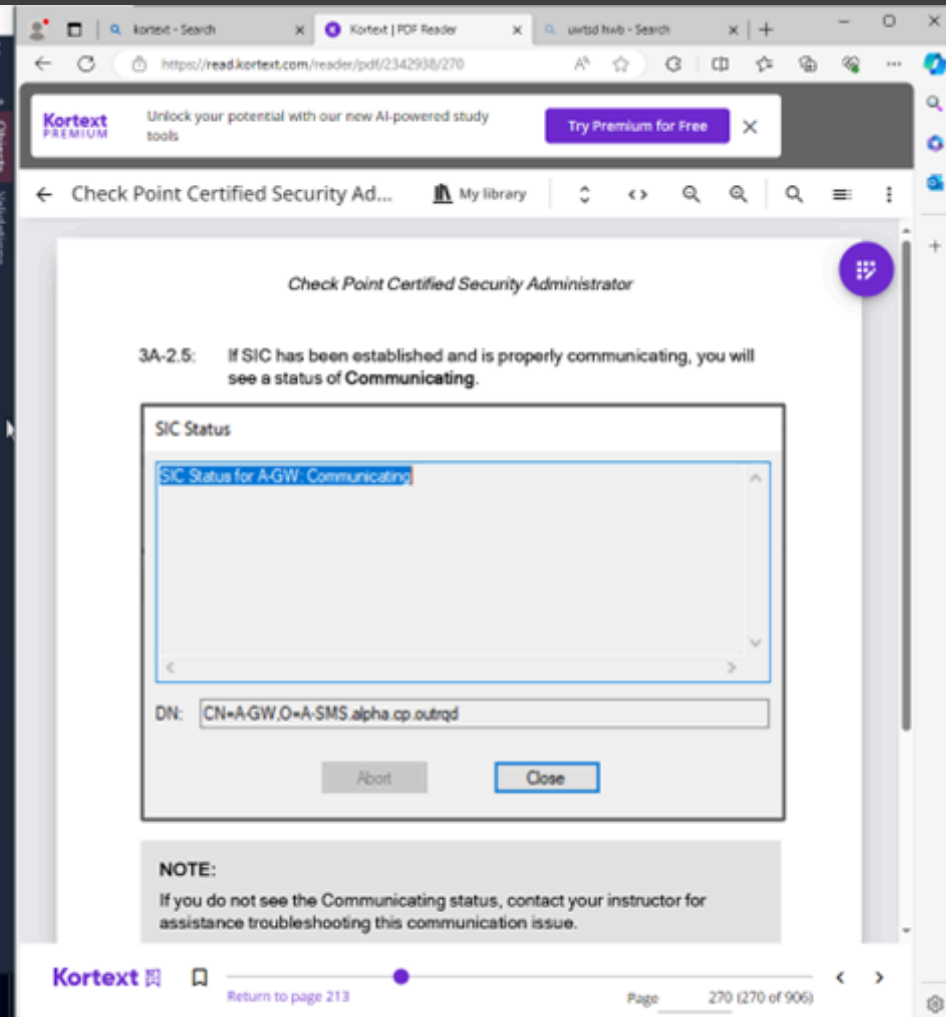
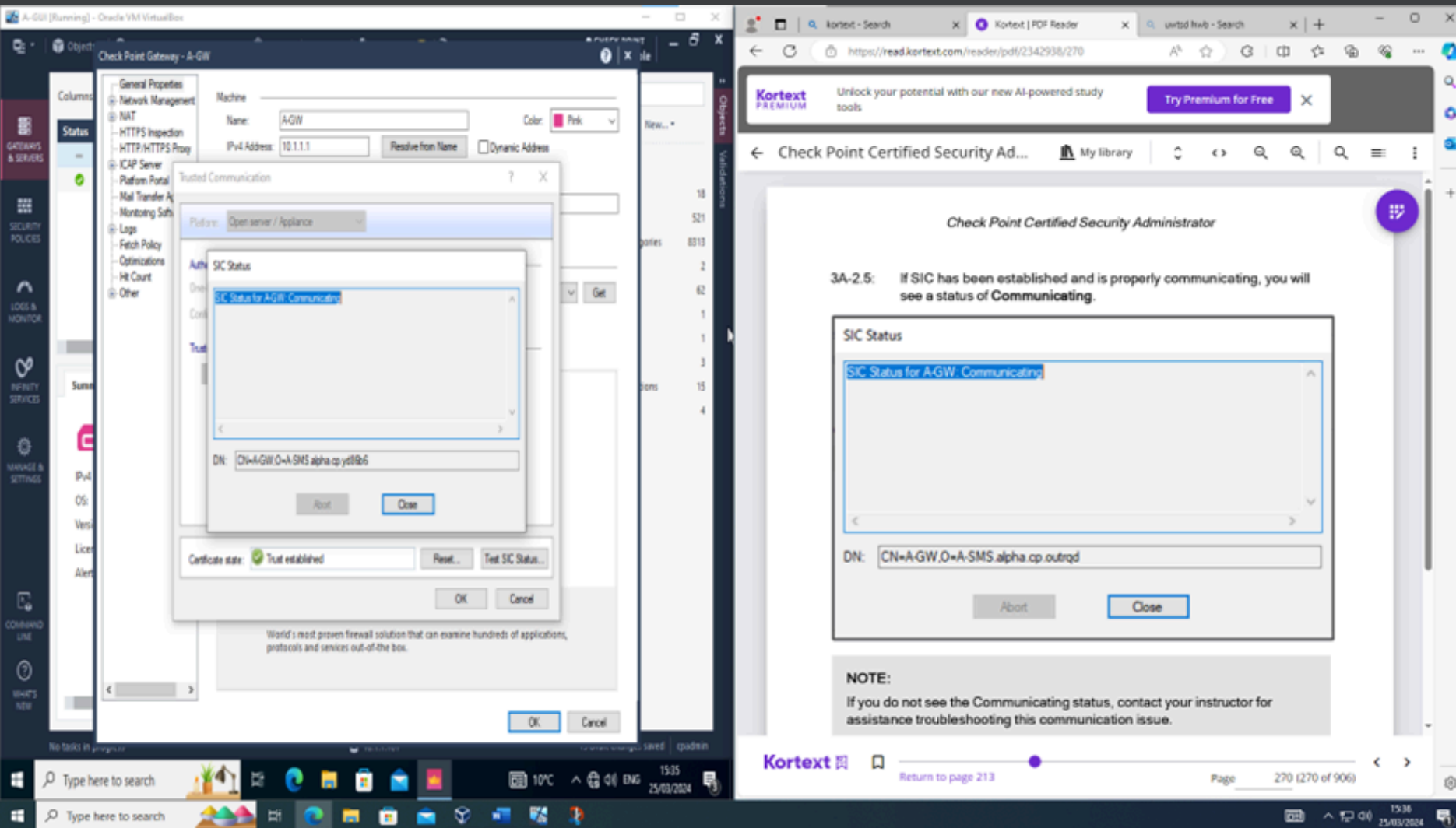
Configuration of a security Management Server



Edited A-SMS color and comment

Lab : Checkpoint security administration

Test of the Secure Internal Communication between A-GW and A-SMS



Creation of the administrator
Baptiste_FAGET

Lab : Managing Administrator access

The image displays two overlapping screenshots of the Check Point SmartConsole interface. The left screenshot shows the 'Sessions' tab with a list of active sessions. The right screenshot shows the 'A-GW' configuration page with a 'SmartConsole' dialog box indicating a session takeover.

Active Session before the taking over

Taking over by administrator

SmartConsole Sessions Table

Name	Administrator	Workflow State
(Current Session)	Baptiste_FAGET	Open (2)
(Unnamed)	cpadmin	Read Write (2)

SmartConsole A-GW Configuration Table

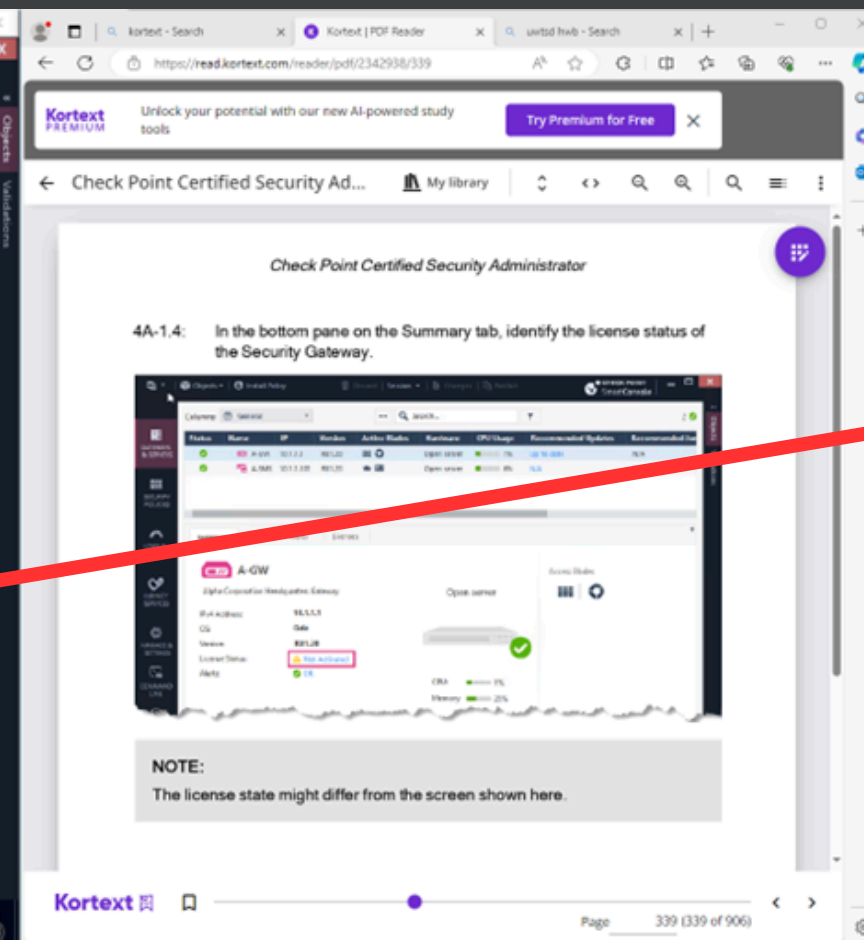
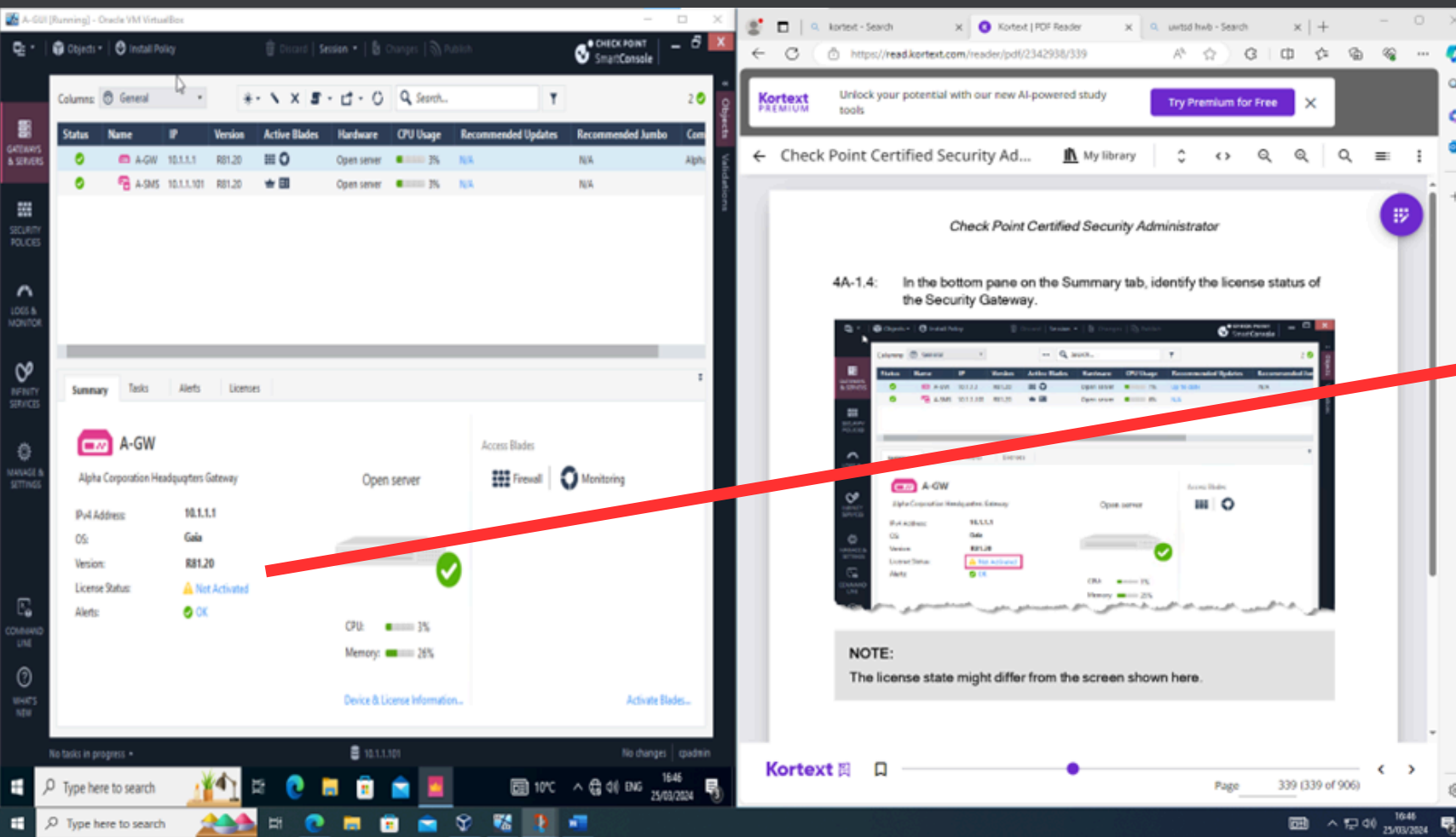
Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommended Jumbo	Comments
✓	A-GW	10.1.1.1	R81.20	✓	Open server	3%	N/A	N/A	Alpha
✓	A-SMS	10.1.1.101	R81.20	✓	Open server	3%	N/A	N/A	

SmartConsole Dialog Box:

! Your session was taken over by administrator Baptiste_FAGET.

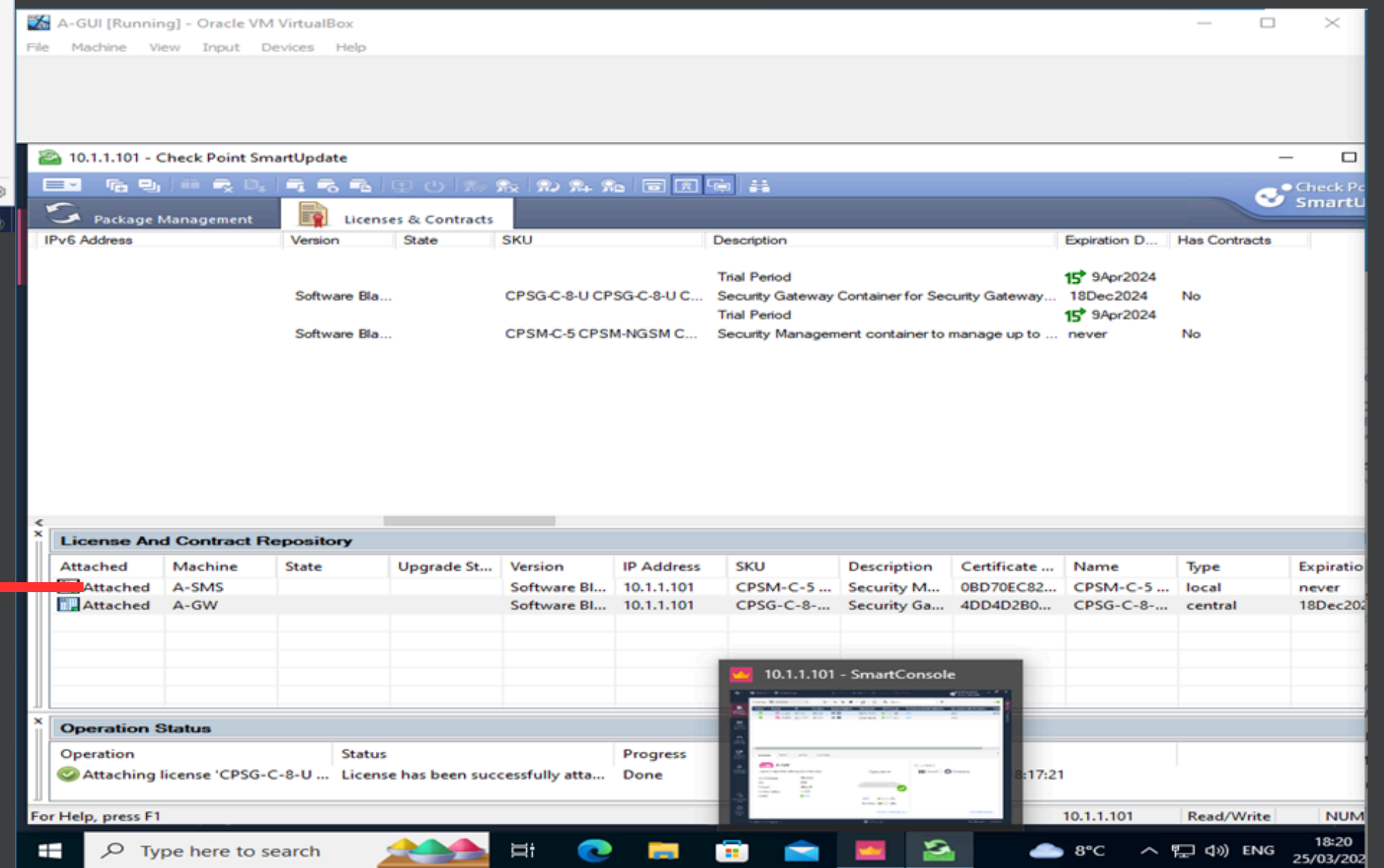
OK

Lab : Checkpoints Licenses



Current licence status

Attachment of licenses to A-SMS
and A-GW



Lab : Managing Licenses

The image shows a virtual machine environment with two main windows. On the left is a terminal window titled 'A-GUI [Running] - Oracle VM VirtualBox'. It displays the output of the 'show license' command, which lists various licenses and their expiration dates. On the right is a PDF viewer window titled 'Kortext | Lecteur PDF', displaying a document titled 'Check Point Certified Security Administrator R81.20'. The document contains a section titled '4A-4.8: Review the attached license and contracts:' which lists the same license information as the terminal window. Red arrows point from the terminal window to the PDF document, indicating the source of the license information.

Terminal Window Output:

```
Host: 10.1.1.101
Expiration: never
Features: CPSP-C-5 CPSP-MOSH CPSP-WKFL-5 CPSP-NPM CPSP-EPH
CPSP-LOOS CPSP-MNTR CPSP-MPTL CPSP-UDIR CPSP-PRVS CPSP-COMP-5 CPSP-SME-5 CPSP-
RPRT-M-C1000 CK-0BD70EC025FC

Contract Coverage:
# ID Expiration SKU
1 | 1443271 | 11Jan2025 | CPSP-EVNT-5-1Y
(Covers: CPSP-C-5 CPSP-MOSH CPSP-WKFL-5 CPSP-NPM CPSP-EPH CPSP-LOOS CPSP-
B-MNTR CPSP-MPTL CPSP-UDIR CPSP-PRVS CPSP-COMP-5 CPSP-SME-5 CPSP-RPRT-M-C1000
CK-0BD70EC025FC)
2 | 28E4AF1 | 11Jan2025 | CPSP-COMP-5-1Y
(Covers: CPSP-C-5 CPSP-MOSH CPSP-WKFL-5 CPSP-NPM CPSP-EPH CPSP-LOOS CPSP-
B-MNTR CPSP-MPTL CPSP-UDIR CPSP-PRVS CPSP-COMP-5 CPSP-SME-5 CPSP-RPRT-M-C1000
CK-0BD70EC025FC)
3 | 101K60D | 11Jan2025 | CPSP-RPRT-5-1Y
(Covers: CPSP-C-5 CPSP-MOSH CPSP-WKFL-5 CPSP-NPM CPSP-EPH CPSP-LOOS CPSP-
B-MNTR CPSP-MPTL CPSP-UDIR CPSP-PRVS CPSP-COMP-5 CPSP-SME-5 CPSP-RPRT-M-C1000
CK-0BD70EC025FC)
A-SMS>
```

PDF Document Content:

4A-4.8: Review the attached license and contracts:

```
# ID Expiration SKU
1 | 1443271 | 11Jan2025 | CPSP-EVNT-5-1Y
(Covers: CPSP-C-5 CPSP-MOSH CPSP-WKFL-5 CPSP-NPM CPSP-EPH CPSP-LOOS CPSP-
B-MNTR CPSP-MPTL CPSP-UDIR CPSP-PRVS CPSP-COMP-5 CPSP-SME-5 CPSP-RPRT-M-C1000
CK-0BD70EC025FC)
2 | 28E4AF1 | 11Jan2025 | CPSP-COMP-5-1Y
(Covers: CPSP-C-5 CPSP-MOSH CPSP-WKFL-5 CPSP-NPM CPSP-EPH CPSP-LOOS CPSP-
B-MNTR CPSP-MPTL CPSP-UDIR CPSP-PRVS CPSP-COMP-5 CPSP-SME-5 CPSP-RPRT-M-C1000
CK-0BD70EC025FC)
3 | 101K60D | 11Jan2025 | CPSP-RPRT-5-1Y
(Covers: CPSP-C-5 CPSP-MOSH CPSP-WKFL-5 CPSP-NPM CPSP-EPH CPSP-LOOS CPSP-
B-MNTR CPSP-MPTL CPSP-UDIR CPSP-PRVS CPSP-COMP-5 CPSP-SME-5 CPSP-RPRT-M-C1000
CK-0BD70EC025FC)
A-SMS>
```

NOTE:
Your license and contracts information might differ.

Licenses

Contrats

Lab : Creating security_policy.

Access control policy:

- Cleanup rule
- Management rules
- Traffic rules

The screenshot shows the Check Point SmartConsole interface. On the left, the 'Install Policy' menu is open, showing options like 'Manage policies and layers...', 'Open Object Explorer...', 'New object', 'Publish session', 'Discard session', 'Session details...', 'Install policy...', 'Verify Access Control Policy...', 'Install database...', 'Uninstall Threat Prevention Policy...', 'Management High Availability...', 'Manage licenses and packages...', 'Search/monitoring...', 'Endpoint', 'View', 'About Check Point SmartConsole...', 'Help', and 'Exit'. The 'Global properties' option is highlighted. On the right, a table lists rules. The 'Cleanup Rule' is highlighted in yellow. A red arrow points from the 'Cleanup Rule' in the table to the 'Global properties' option in the 'Install Policy' menu.

No.	Name	Source	Destination	VPN
1	Noise Rule	* Any	* Any	* Any
2	Recommend Cleanup Rule	* Any	* Any	* Any
3	Update Rule	A-SMS	* Any	* Any
4	Management Rule	A-RASAT.NET	A-GW	* Any
5	Stealth Rule	* Any	A-GW	* Any
6	Drop Rule	Alpha Networks	* Any	* Any
7	Drop Rule	* Any	A-CMZ	* Any
8	Drop Rule	Alpha Networks	* Any	* Any

Stealth rule is use to drop traffic not allowed by the firewall.

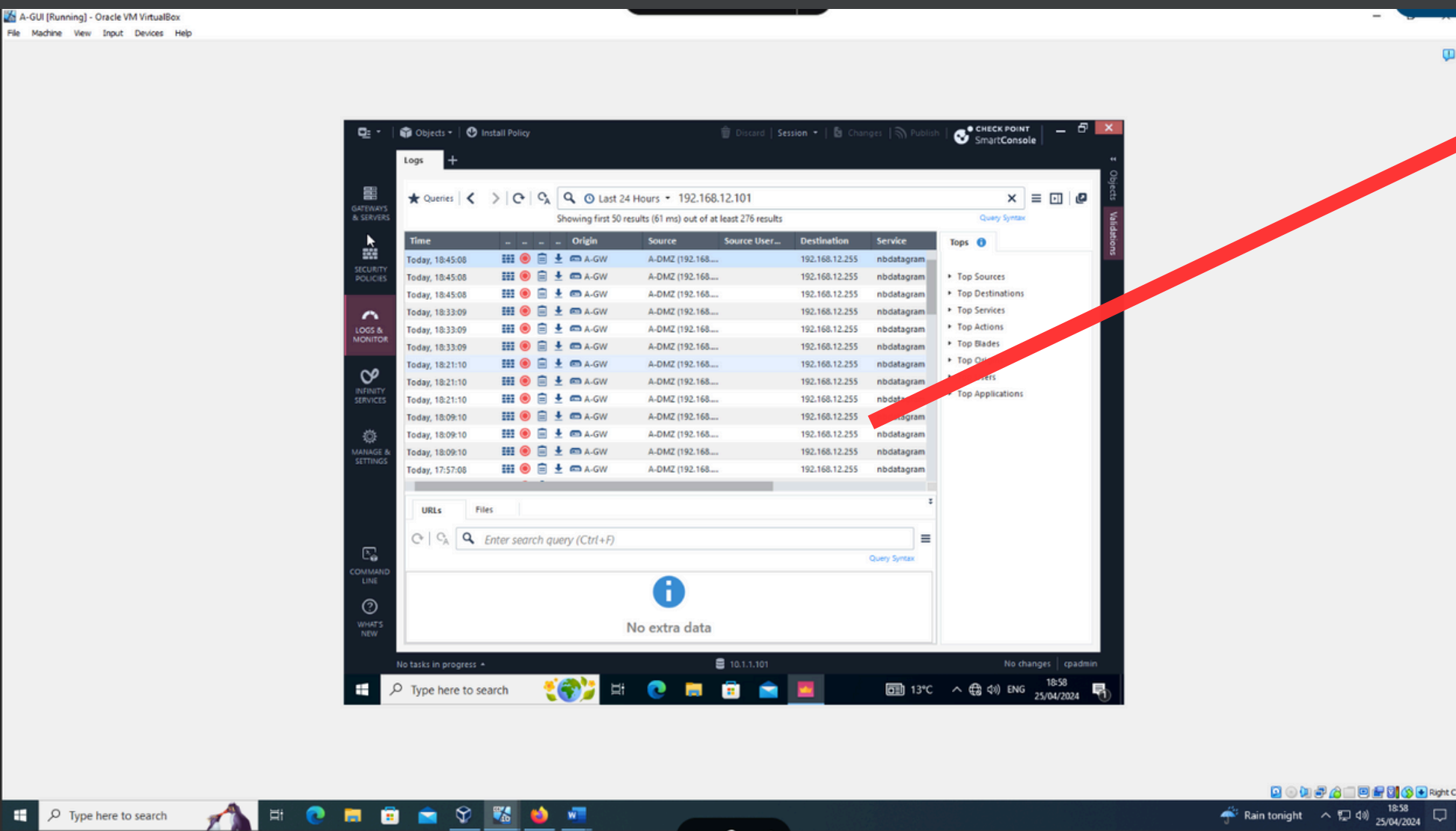
Cleanup rule determine how to handle connections not match by the rule.

Lab : Installing security_policy.

The image displays two side-by-side screenshots. The left screenshot shows the Check Point SmartConsole interface with the 'Install Policy' window open. The window shows the policy installation details, including the time (Today 16:55:54), type (Audit), application (SmartConsole), and administrator (cpadmin). The right screenshot shows a PDF document titled 'Check Point Certified Security Administrator R81.20' with a red arrow pointing from the 'Log of the most recent install policy' text to the 'Log Info' section of the 'Install Policy' window in the SmartConsole. The PDF also contains instructions for selecting audit logs and viewing log details.

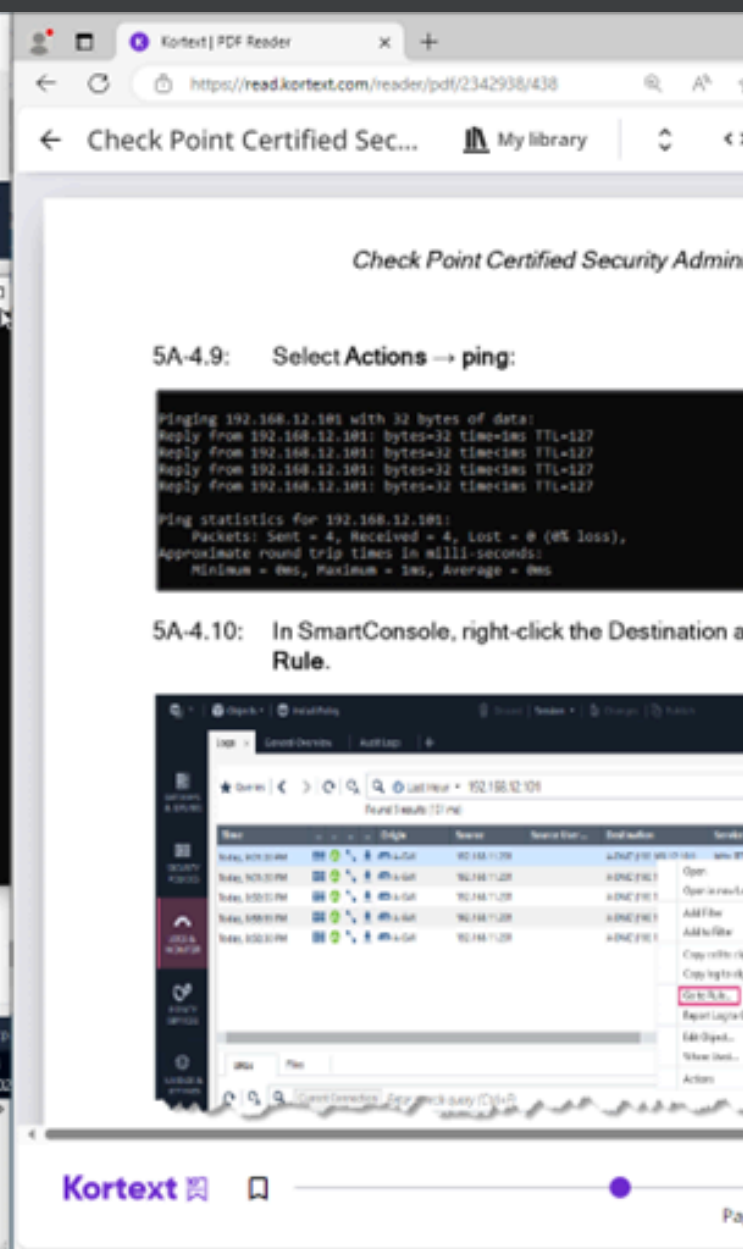
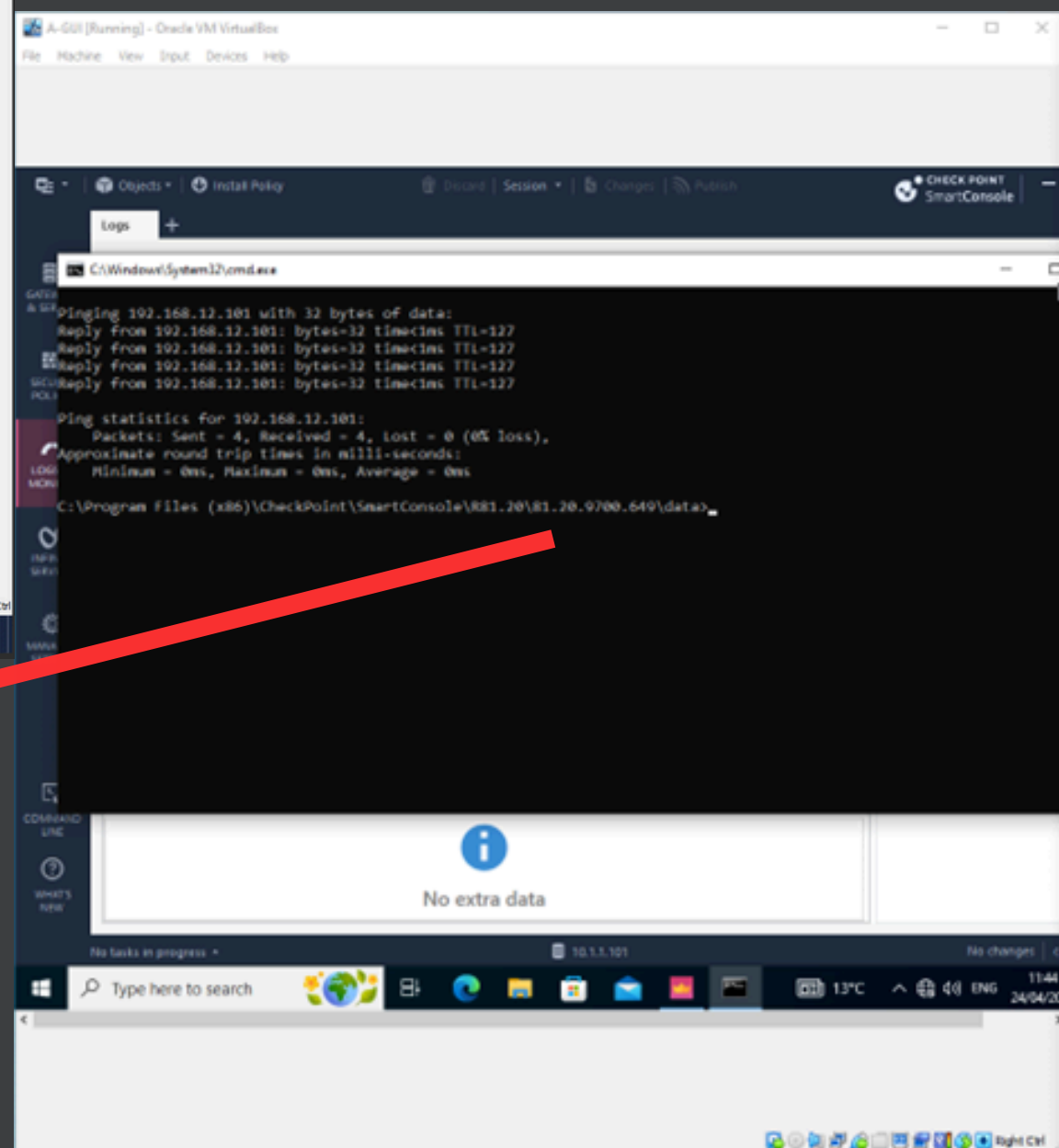
Log of the most recent install policy

Lab : Testing the standard security policy.

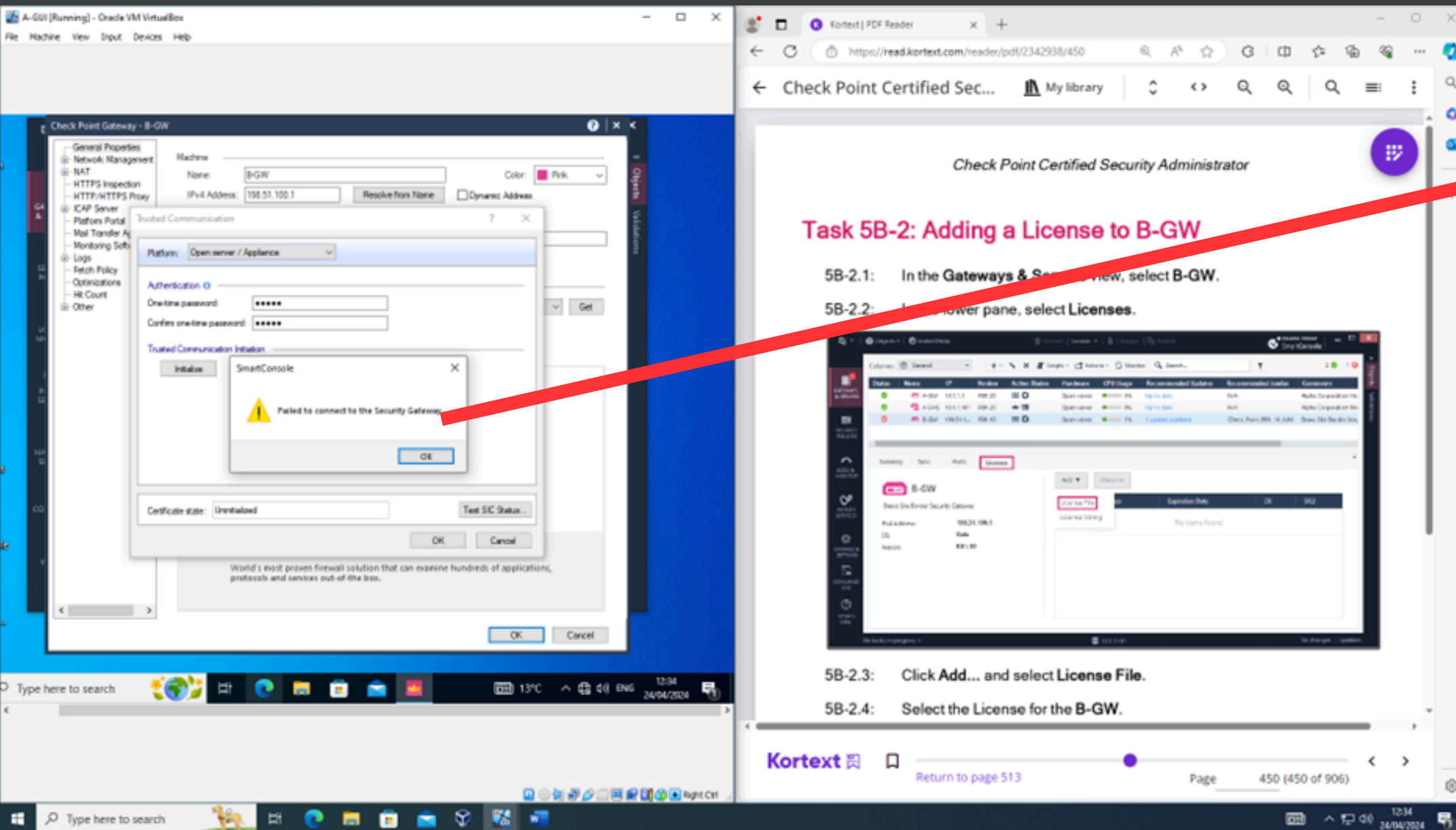


Log of connection in A-DMZ

Succed ping between



Lab : Creating Bravo Security Policy.



Failed to connect the security gateway.

Lab : Configuring Order Layers

The image is a collage of screenshots from a Check Point SmartConsole and a web browser, illustrating the configuration of web control layers and the attempt to access Facebook.com.

Check Point SmartConsole Screenshots:

- Policy Configuration:** A screenshot of the SmartConsole interface showing the configuration of a policy. The "Web Content Layer" is selected, and a rule is being configured. The rule's destination is set to "Alpha Networks".
- Policy Details:** A screenshot showing the "Details" tab of the policy configuration. The "Destination" is set to "Alpha Networks".
- Policy Summary:** A screenshot showing the "Summary" tab of the policy configuration. The "Destination" is set to "Alpha Networks".
- Policy Logs:** A screenshot showing the "Logs" tab of the policy configuration. The logs show traffic from "Alpha Networks" to "Internet".

Web Browser Screenshots:

- Check Point Certified Security Administrator:** A screenshot of the Check Point Certified Security Administrator web page. A red arrow points from the "Web Content Layer" in the SmartConsole to this page, with the text "Installing web control layers".
- Web App Blocker:** A screenshot of the Web App Blocker web page. A red arrow points from the "Web Content Layer" in the SmartConsole to this page, with the text "Web App Blocker".
- Facebook.com:** A screenshot of the Facebook.com login page. A red arrow points from the "Log that we try to go on Facebook.com" text to this page.

Other Screenshots:

- Important!:** A screenshot showing an important message: "By negating the Destination portion of the rule, we are configuring the policy to drop any traffic that contains PCI information that is sent to OTHER THAN those identified by Alpha-Networks or B-INT".
- 6A-2.9:** A screenshot showing the instruction: "Verify the rules are configured correctly by comparing the following figure:".
- 6A-2.10:** A screenshot showing the instruction: "Publish the changes."
- Download our new video editor:** A screenshot showing a notification for a new video editor.
- Logs:** A screenshot showing the logs of the policy configuration. The logs show traffic from "Alpha Networks" to "Internet".

Reccomandation for future improvement

- Add redundancy to avoid single points of failure.
- Encrypt the data : Add some crypsis with public and private key to enhance the security,
- Implement a virtualized network architecture: Network virtualization can help improve network agility and flexibility

Personnal and Technical reflection

- Personnal Reflections:
 - User friendly.
 - Well documented, appreciate the explanation before the lab.
- Technical reflection :
 - The Check Point application offers centralized security management, enabling administrators to manage the security of the entire network.
 - Check Point is designed to be scalable and can support networks of all sizes, from small businesses to large enterprises.

Conclusion

During these various practical works, we were able to significantly improve the security of TG Entreprise. Thanks to the Checkpoint tool, we were able to:

- Add security rules for both users and the network
- Create multiple levels of administrator
- Attach licenses and contracts that allow us to generate regular reports.

Through these actions, we have strengthened the protection of TG Entreprise's network and improved our ability to monitor and manage security threats. The implementation of Checkpoint has provided us with a powerful and comprehensive security solution that meets the needs of our organizatio