

Portfolio (Part 3): Analysis, Design, and Implementation of a Network Security Solution

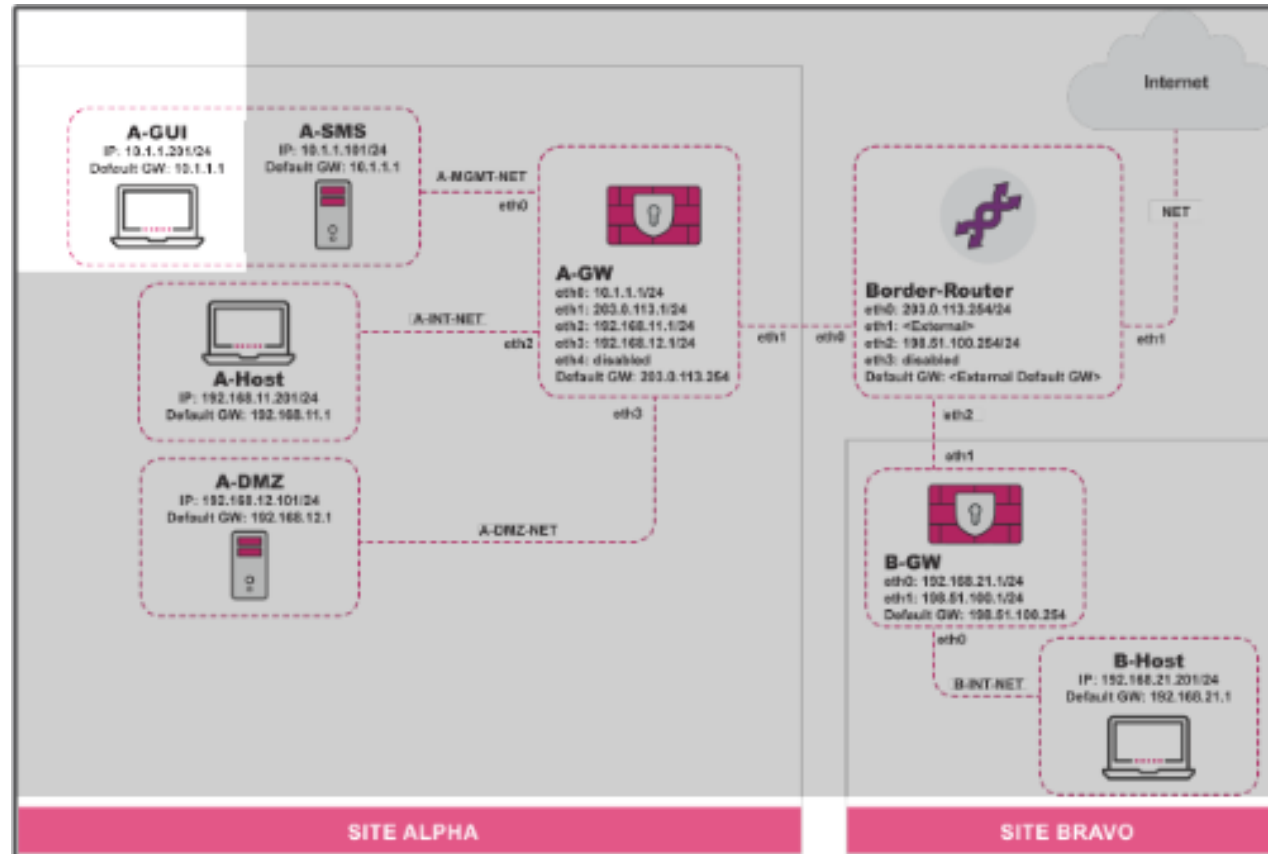
Tinnin Hassan

2325677@student.uwtsd.ac.uk

Synopsis

- I. Analysis on the existing security posture based on the critical issues
- II. Implementation details with adequate screenshots including a demo and any challenges faced during the deployment of the Checkpoint security solution.
- III. Implementation of any additional security features benchmarking industry standards.
- IV. Recommendations for future improvements based on the lessons learned during the implementation and analysis process.
- V. Personal and Technical Reflection.
- VI. Conclusion

Initial topology



Initial topology

Analysis of the existing security posture based on the critical issues.

Irregular Security Audits and Updates

- **Issue:** expose to potential vulnerabilities and outdated security configuration.
- **Assumption:** . There may be resource constraints or a lack of dedicated personnel.
- **Solution:** Check Point's Security Management platform to automate security audits and updates.

Single Points of Failure

- **Issue:** Presence of single points of failure compromises network availability and resilience.
- **Assumption:** Critical components such as firewalls are deployed without redundancy measures, leading to potential disruptions.
- **Solution:** Configure clustering and redundancy to ensure continuous operation.

Inconsistencies and Errors in Policy Management

- **Issue:** Inefficiencies in policy management result in inconsistencies and errors
- **Assumption:** due to manual processes or lack of standardized procedures.
- **Solution:** Check Point's SmartConsole for centralized policy management

Licensing Structure

- **Issue:** Current licensing structure is costly and includes unnecessary features.
- **Assumption:** Check Point licenses are not optimized to align with specific security requirements, leading to unnecessary expenses.
- **Solution:** Conduct a license review

User Roles and Permissions

- **Issue:** Undefined roles and permissions contribute to unauthorized access.
- **Assumption:** lacks a well-defined Role-Based Access Control (RBAC) framework, resulting in excessive privileges in access controls.
- **Solution:** Implement it using Check Point's security management architecture.

Analysis of the existing security posture based on the critical issues.

Overlapping and Conflicting Policies

- **Issue:** Overlapping and conflicting security policies
- **Assumption:** Legacy configurations or multiple administrators managing security settings independently lead to redundant policies and conflicts.
- **Solution:** Check Point's Policy Optimizer tool to analyze and streamline security policies

Lack of Control Over Application Usage

- **Issue:** UP
- **Assumption:** TG Enterprise has limited visibility and control over the applications used within the network, leading to security risks and compliance issues.
- **Solution:** Deploy Check Point's Application Control and URL Filtering features

Outdated IPS Rules

- **Issue:** It diminishing the effectiveness of intrusion prevention.
- **Assumption:** Enterprise lacks automated processes for updating IPS rules
- **Solution:** Enable automatic updates and real-time threat intelligence using Check Point's ThreatCloud database. Regularly update IPS rules to protect against emerging threats.

Challenges Posed by IoT Devices

- **Issue:** UP
- **Assumption:** struggles to secure IoT devices due to the complexity of managing diverse endpoints and the lack of specialized security measures for IoT deployments.
- **Solution:** Use network segmentation and device profiling to secure IoT deployments effectively.

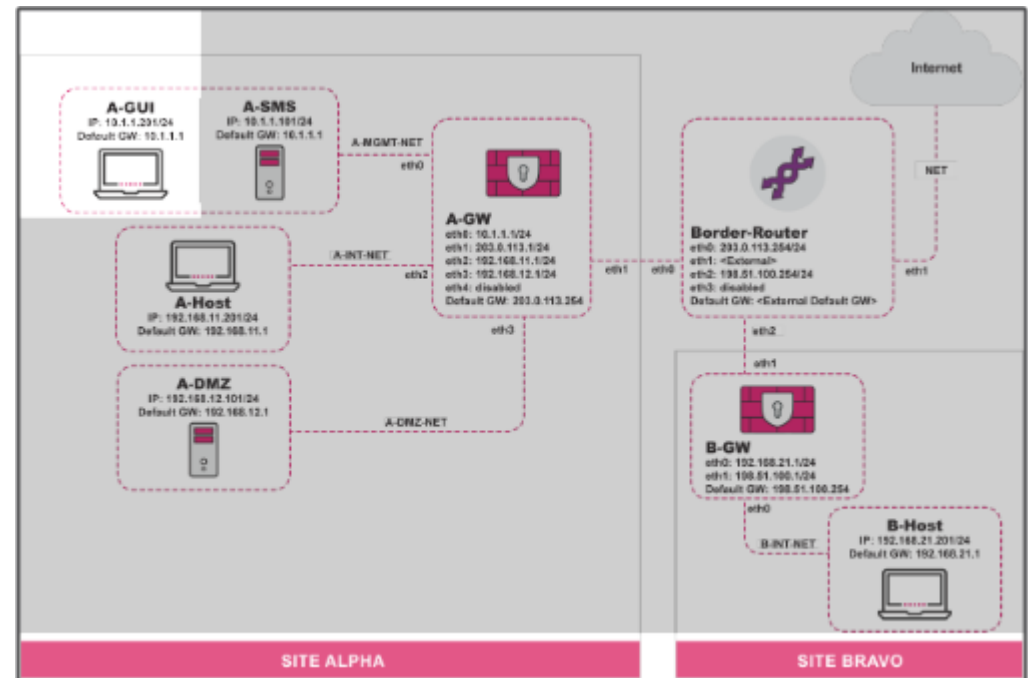
Implementation of the lab topology

Objectives and outcomes:

- Network Security Students has basics knowledge of the fundamentals of network security, for some of them even some experience.
- However, every company has his own security framework and tools.
- Checkpoint is a pionnier in the domain of network security. Today, Checkpoint is in the top 8 Enterprise Networking Security companies next to Cisco, Fortinet, Palo alto which has been created by an former Checkpoint Engineer.
- The Check Point Security Administration (CCSA) course covers the fundamentals to manage Checkpoint Security Gateways and Management Software Blades that run in their Gaia OS.
- I start this work with the intention to help orthers by understanding the checkpoint network security framework and tools.
- My goal was to get used to about how to manage an cyber-security platform.
- Finally, I did almost all the tasks until the Lab 6A-3.

Implementation of the lab topology

- 1) *Deploying SmartConsole*
- 2) *Installing Primary Security Management Server / installing a security gateway / Configuring Objects in SmartConsole*
- 3) *Establishi Secure Internal Communication / Managing Administrator Access*
- 4) *Managing Licences*
- 5) *Creating Alpha and Beta security Policy*
- 6) *Configuring Policy Layers*



Lab Initial topology

Implementation of the lab topology

- Adequate Screenshots with clarity and Timestamp :

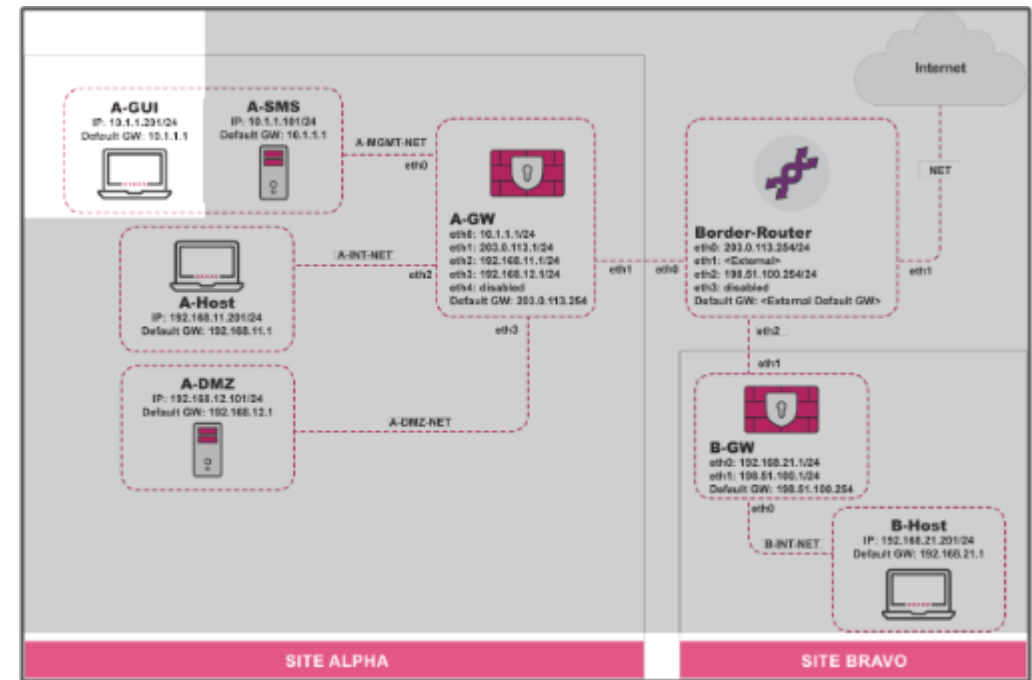
[Lab Screenshots .pdf](#)

- Demo of the current licensing aspect

[demo 1.mp4](#)

- Demo of additional security features benchmarking industry standards. : [demo 2](#)

- Challenges: Troubleshooting issues / need best practices to resolve them and teams breaks



Lab Initial opology

Implementation of the lab topology

Demonstration on the licensing structure (demo on page 8):

- [Checkpoint Licence guide](#)
- License structure: scalable and modular. Ckpt uses predefined packages with the ability to be customized to the need. Thanks to **software blades** (physical blade server) and **container** (physical server chassis) / **Central** and **individual** licensing
- Hardware and Licensing model : depend on the **model**, **nb of gateways**, **nb of users** or **per devices**
- Improvement points: The **A-SMS licence** is a security management container license to manage up to 5 firewalls = **9 saved licences** / So for the **blades** (url filtering, anti-virus, aspm ..) = **18 licenses** / **SSL Network extender**: unlimited (**save of a lot of money...**) / **CPSPB-IPSI** (small business ?)

Implementation of any additional security features benchmarking industry standards

Objectives and outcomes:

- **ISO/IEC 27001:** (International organization for standardization) / (International Electrotechnical Commission) standards. Revised in 2022.
- Annex **A.9.4: safeguard** access to information and **ensure** that employees can only view information that's relevant to their work.
- Divided into 4 **four sections:** Access Controls, User Access Management, User Responsibilities and Application Access Controls.
- Annex A.9.4: **Prevent unauthorised access to systems and applications.**
- **Objectives:** Create a unified layer / Integrate it with multiples access blades / Build a unified policy.
The demo is on page 8

Recommendations and reflections

Recommendations

- Make team breaks to permit to the teacher to explain to everyone how to troubleshoots the mains problems rather that explain it 10 times

Personnal and technical Reflections

- Personal : learn about a main actor into the cybersecurity industry
- Technical: learn about how to use a security platform

Conclusion

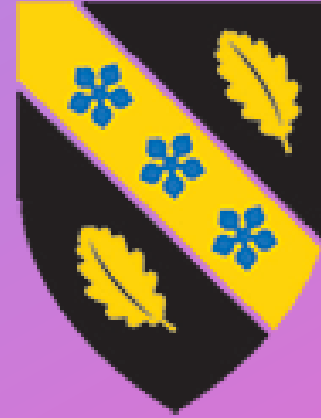
Recommandations

- Make team breaks to permit to the teacher to explain to everyone how to troubleshoots the mains problems rather that explain it 10 times

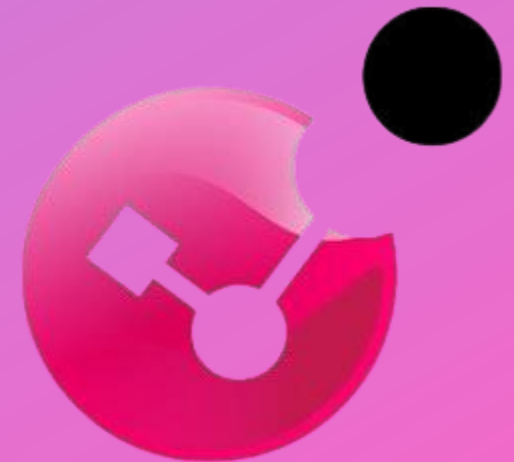
Personnal and technical Reflections

- Personal : learn about a main actor into the cybersecurity industry
- Technical: learn about how to use a security platform

Conclusion



CHECK POINT™



Queries ? : Tinnin Hassan / 2325677@student.uwtsd.ac.uk