

May 11, 2024

ANALYSIS, DESIGN AND IMPLEMENTATION OF A NETWORK SECURITY SOLUTION

Module: Enterprise Network Security (ACCA7032)

LECTURER

Munyaradzi Murira

INTERNAL VERIFIER

Nitheesh Kaliyamurthy

STUDENT

Sarah Valery (2325508)



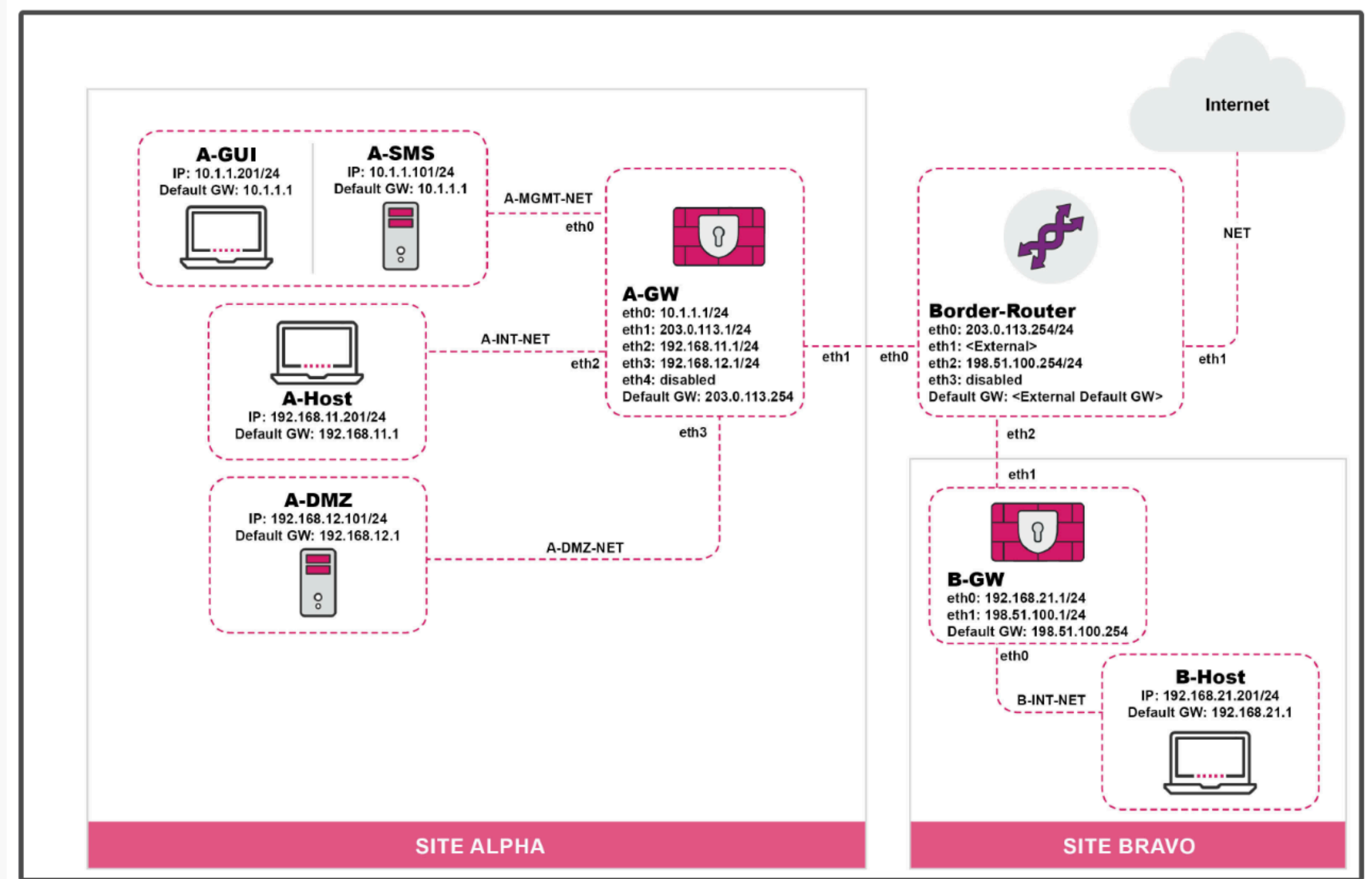
TABLE OF CONTENTS

- 01 Introduction
- 02 Existing security posture analysis
- 03 Implementation:
 - A - Users role and permissions
 - B - Security policies
- 04 Additional implementation: more rules to security policy
- 05 Recommendations for future improvements
- 06 Personal and technical reflection
- 07 Conclusion



01 - INTRODUCTION

- Working for TG Enterprise
- Goal: Enhance their security infrastructure, address their current vulnerabilities, and implement robust security measures that safeguard against both existing and emerging threats



CONTEXT

INITIAL TOPOLOGY

02 - CRITICAL ISSUES ANALYSIS (1/2)

- **Irregular security audits**

- Allows vulnerabilities to persist undetected in crucial areas (ex: DMZ, management interfaces) => Increasing the risk of security breaches.

- **Irregular security updates**

- Essential network components such as the border router and site-specific gateways do not receive timely updates => Exposes the entire network to known vulnerabilities.

- **Single points of failure**

- Border router and gateways represent significant risks if compromised => Any failure here not only jeopardizes external connectivity but also disrupts the entire network's operational capabilities.

- **Inconsistencies and errors**

- Manual configurations of the topology can lead to errors, especially when updating settings across different locations => These inconsistencies can weaken network defenses and complicate the enforcement of unified security policies across all sites.

- **Licensing structure**

- The existing licenses may not adequately cover all the critical areas or might include unnecessary features for certain parts of the network (ex: over-licensing at less critical nodes) => Resources misallocation, where essential areas might be under-protected while less critical areas waste financial resources.

- **User roles and permissions**

- Undefined roles and unclear permissions across the network interfaces and management platforms lead to potential unauthorized access => Increases the risk of internal threats and data breaches.

- **Overlapping and conflicting policies**

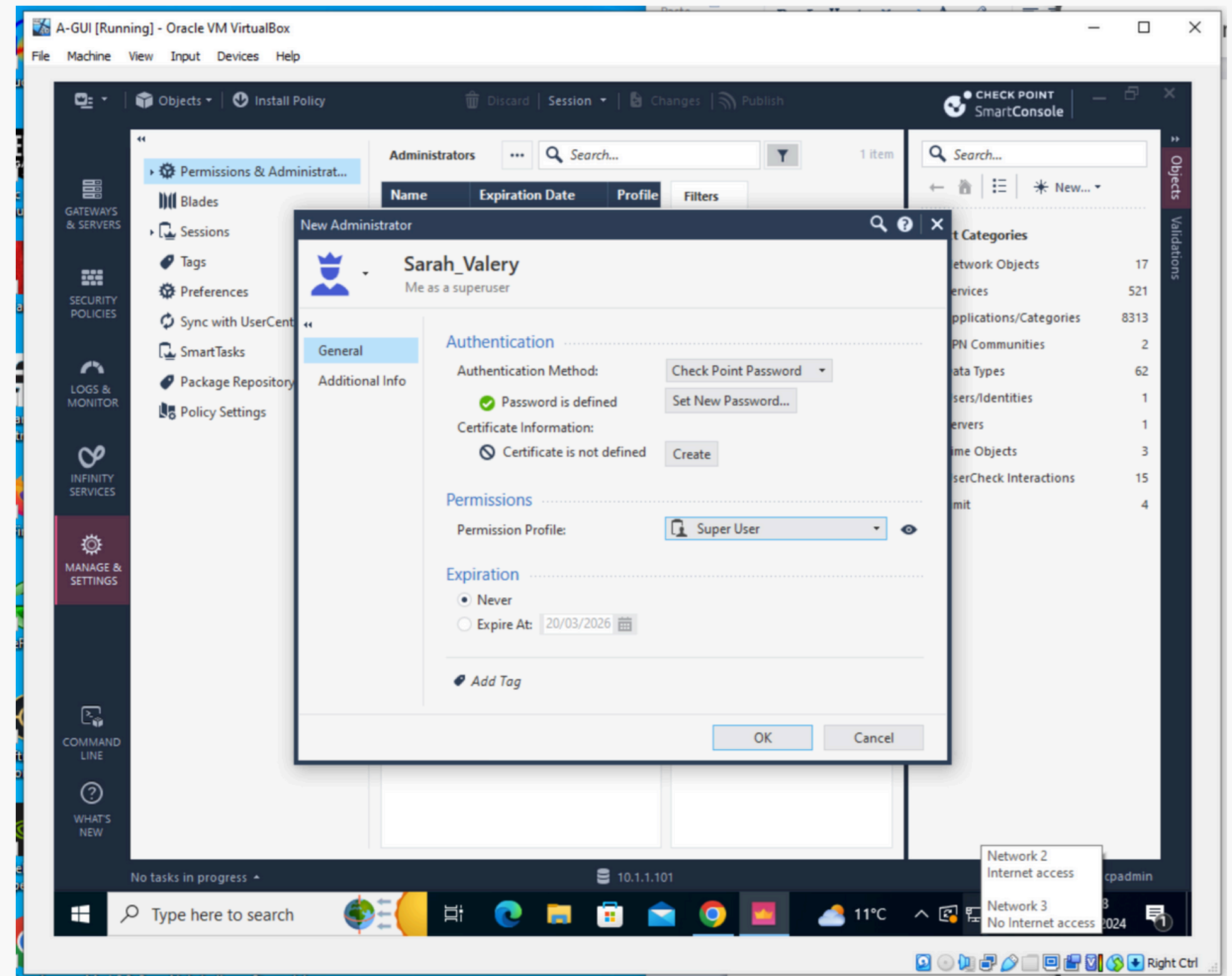
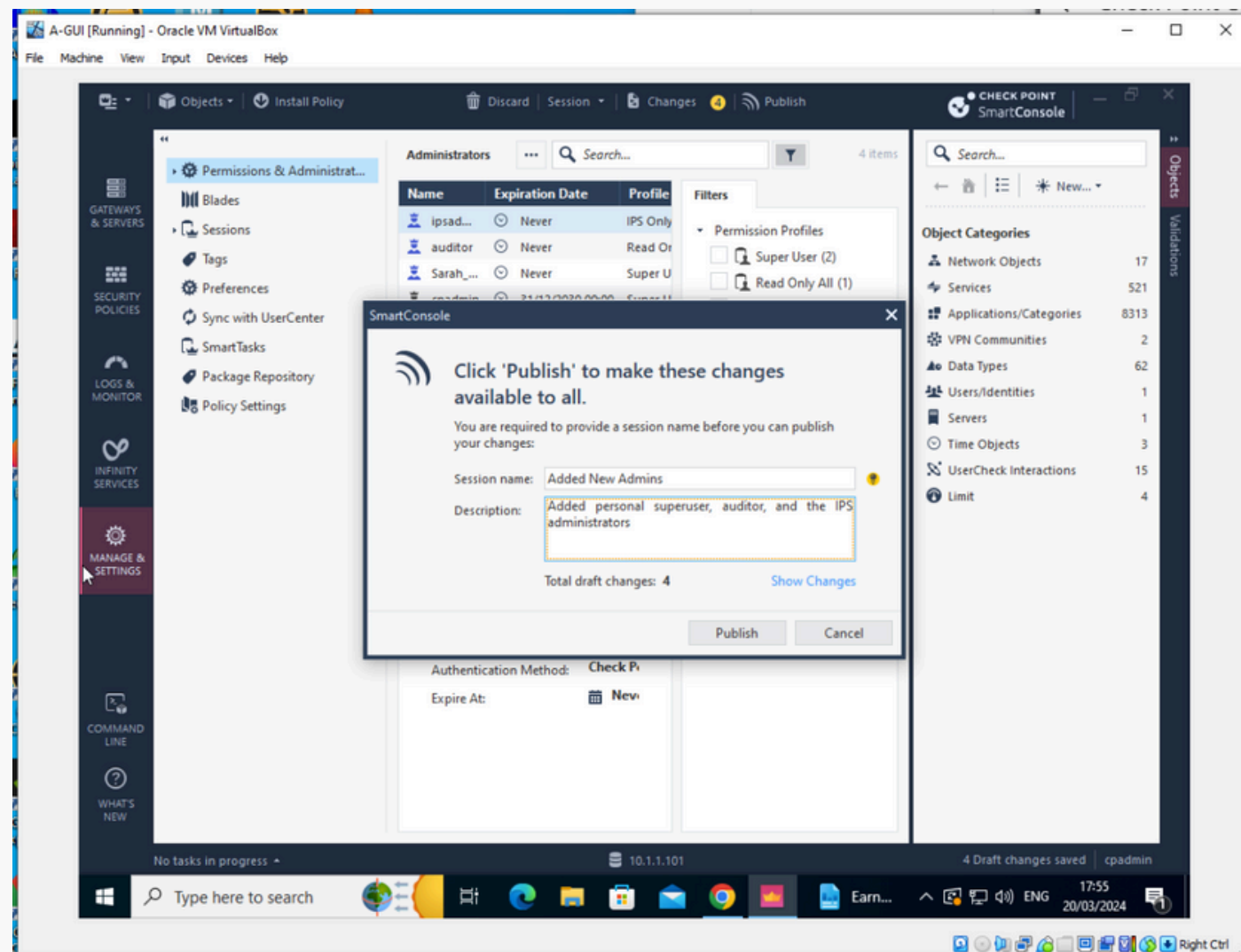
- The policies governing network security across different sites and the border router may overlap or contradict each other => Lead to gaps in the network's defense mechanisms, making it challenging to effectively manage and mitigate attacks.

02 - CRITICAL ISSUES ANALYSIS (2/2)

- **Lack of control over application usage**
 - Inadequate controls over applications running on network hosts and in the DMZ can lead to security vulnerabilities => Opens the network to malware infections and unauthorized data access, particularly in less monitored areas like the DMZ.
- **Outdated IPS rules**
 - If the Intrusion Prevention System rules are not consistently updated across the network's critical junctures => Leads to ineffective threat detection and prevention, particularly harmful in high-risk areas such as the DMZ and border router interfaces.
- **Challenges posed by IoT devices**
 - IoT devices connected across the network, including those in operational environments at both sites, lack standardized security measures => These devices become easy targets for attackers, potentially compromising the broader network.

03 - IMPLEMENTATION: A - USERS ROLES & PERMISSIONS (1/2)

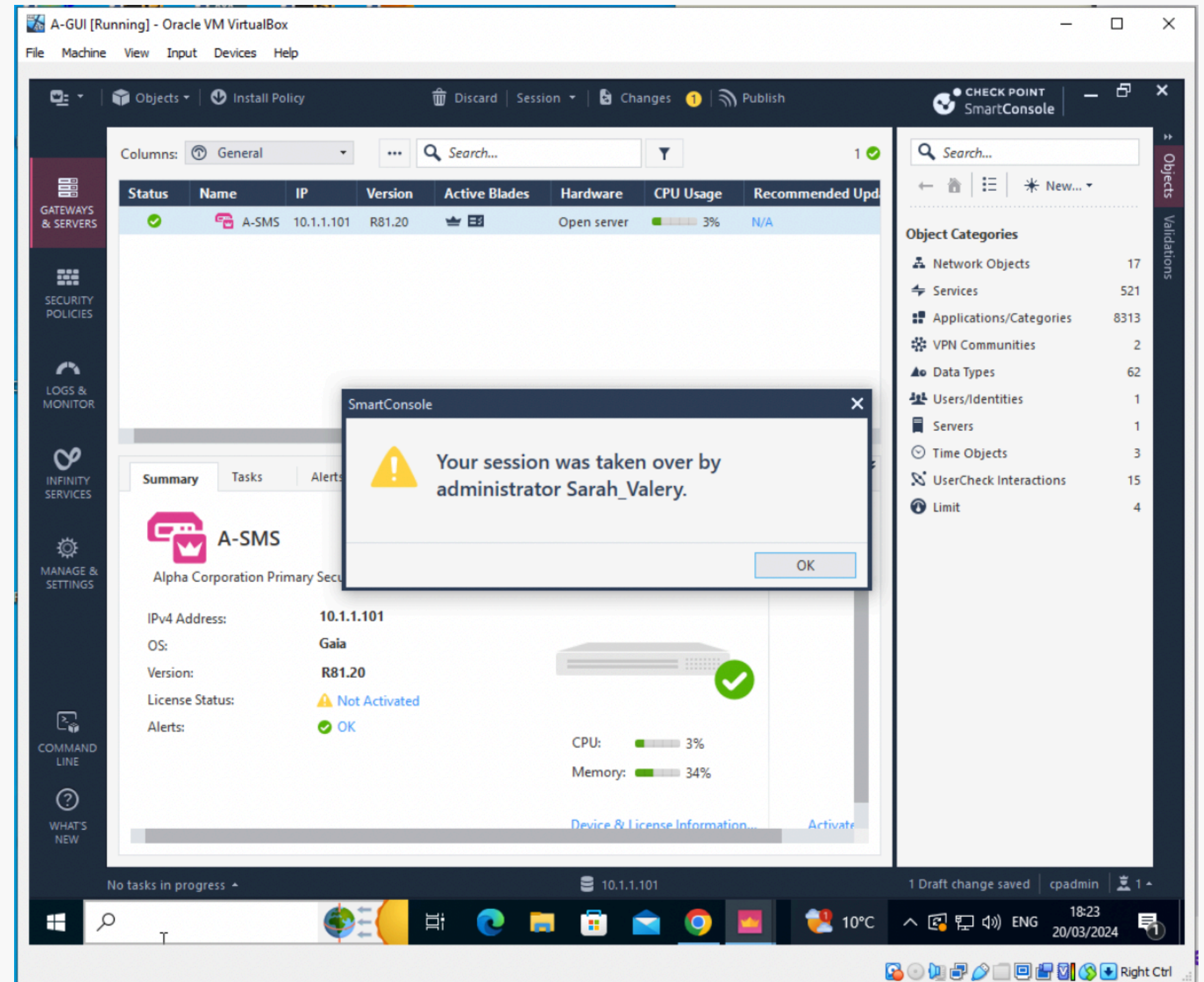
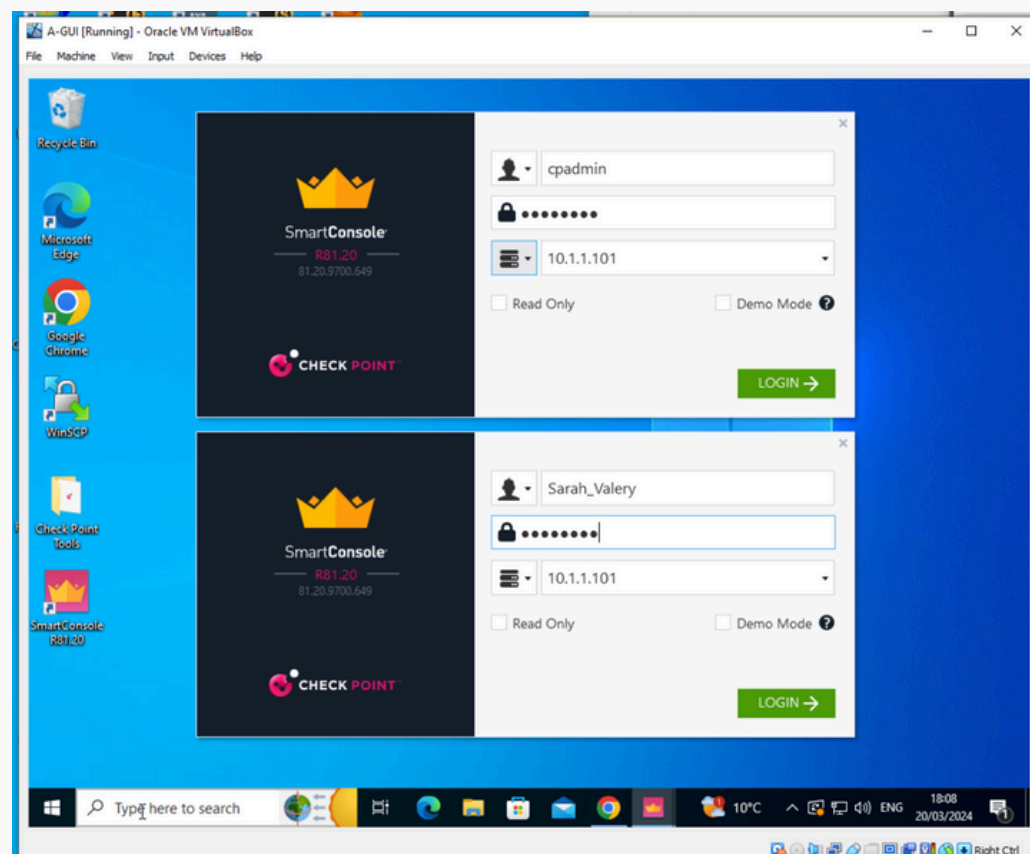
- Created three new users with different role and permissions
 - Sarah Valery = Super User
 - auditor = Read Only All
 - ipsadmin = IPS Only (Customize permission profile)



(Video - 5:40 - 5:50)

03 - IMPLEMENTATION: A - USERS ROLES & PERMISSIONS (2/2)

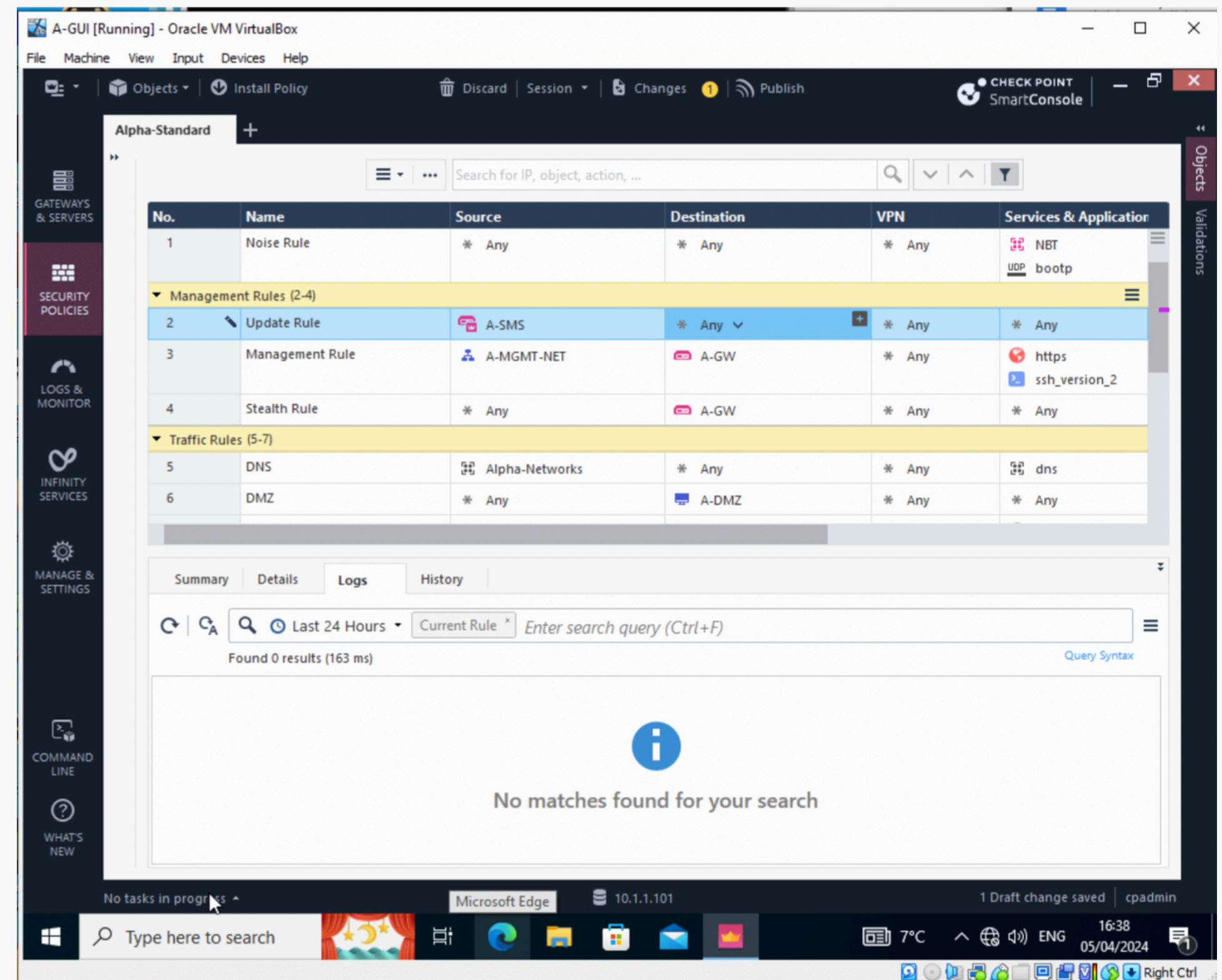
- Managing concurrent administrator sessions
 - Modification made by an administrator is locked for other users to avoid double modification from them
- Taking over another administrator's session
 - "Sarah Valery" taking over "cpadmin" session



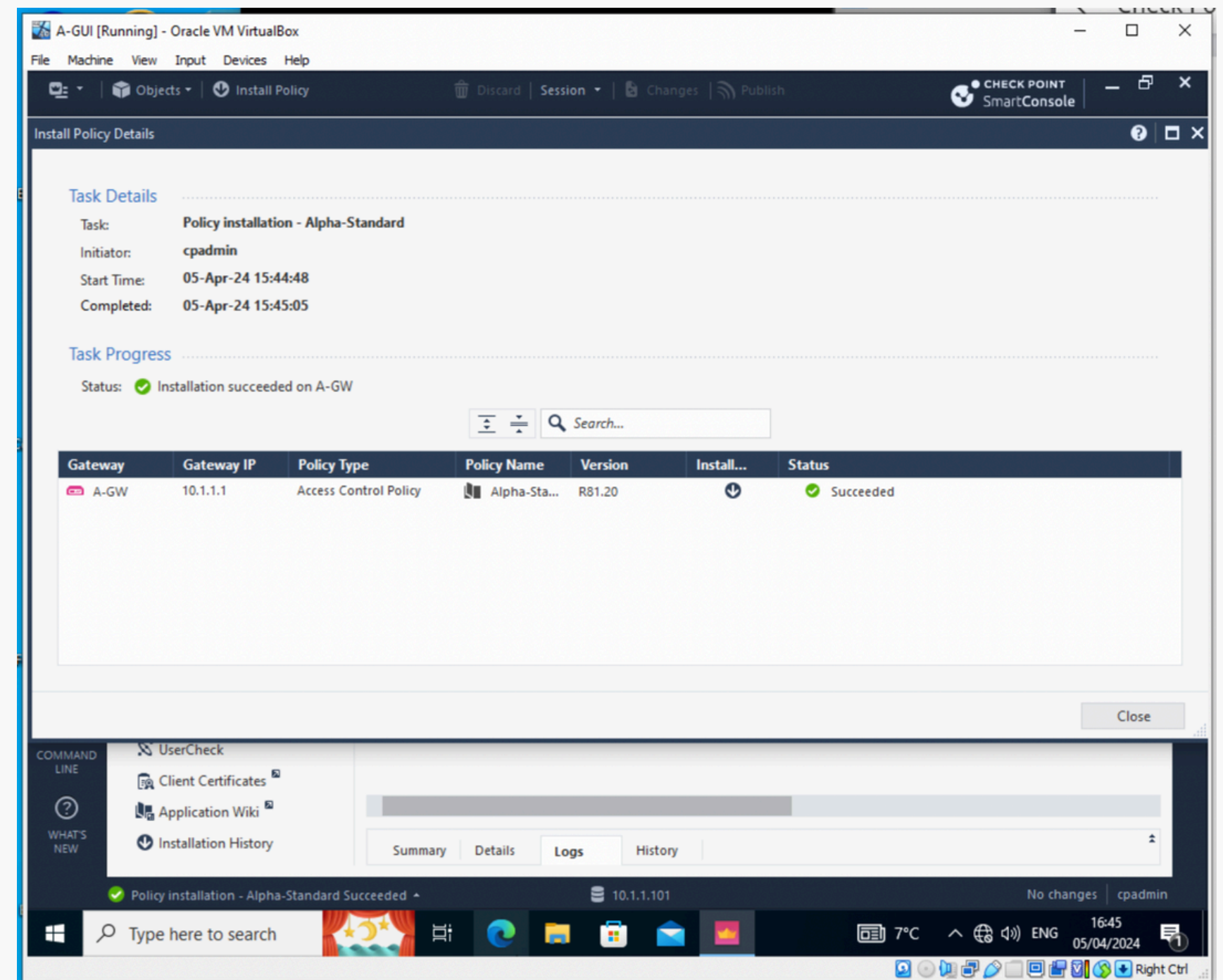
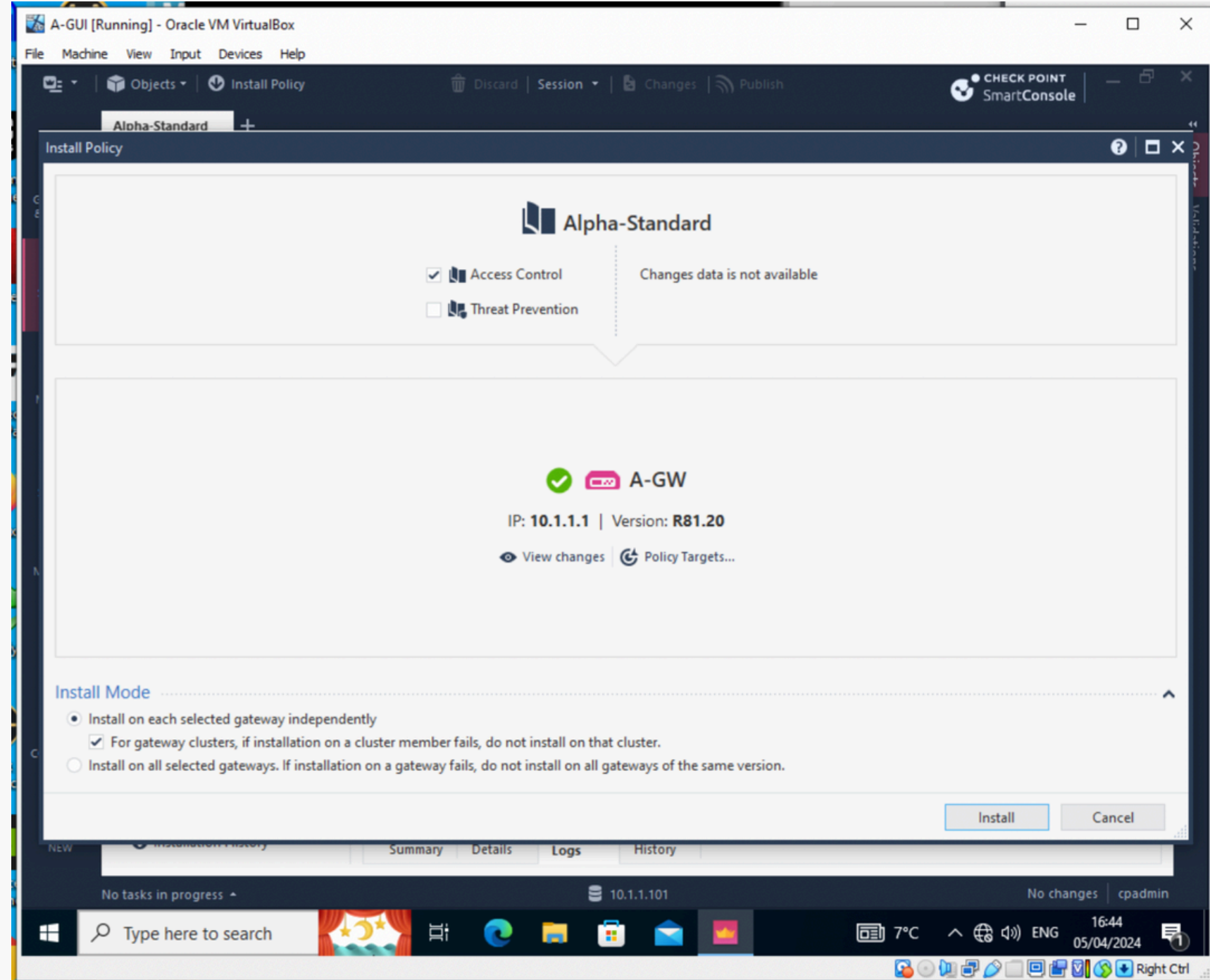
(Video - 5:58)

03 - IMPLEMENTATION: B - SECURITY POLICIES (1/3)

- Created policy objects:
 - Alpha-Standard = Alpha corporation border gateway policy, attached to A-GW
 - B-GW = Bravo site security gateway
 - A-MGNT-NET = Alpha site security management network
 - A-INT-NET = Alpha site internal network
 - A-DMZ = Alpha site DMZ web server
 - Alpha-Networks = Alpha site networks and hosts
- Created standard security policy:
 - 8 rules
- Installing the standard security policy
- Testing the standard security policy
 - Unfortunately not working, address not found even if A-Host is working

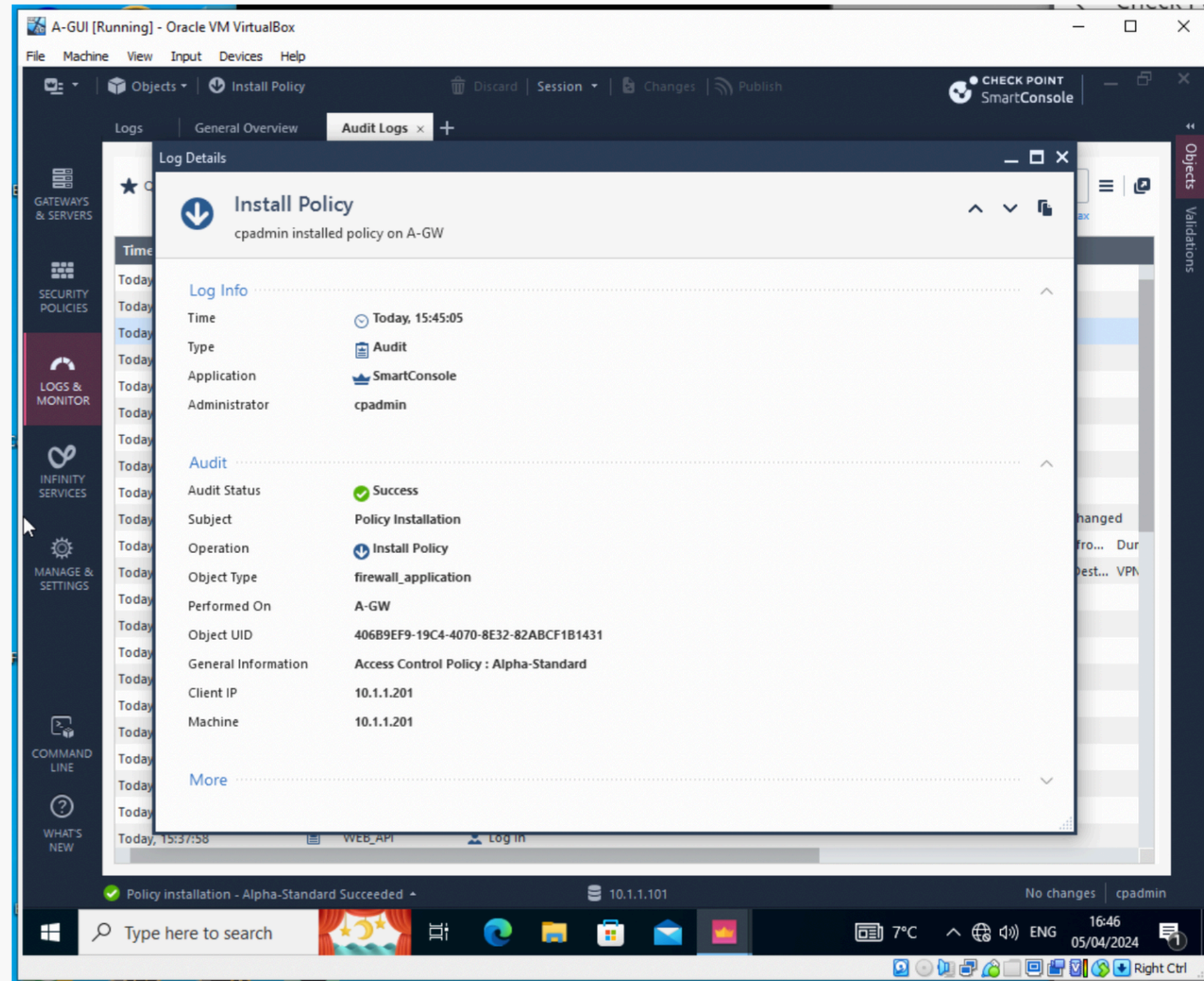


03 - IMPLEMENTATION: B - SECURITY POLICIES (2/3)



03 - IMPLEMENTATION:

B - SECURITY POLICIES (3/3)



04 - ADDITIONAL IMPLEMENTATION: MORE RULES TO SECURITY POLICIES (2/2)

Name	Purpose	Enhancement
SSH Access Control Rule	Controls SSH traffic within the network, ensuring that only authorized nodes can initiate SSH connections. This is particularly important for protecting against unauthorized remote control or data exfiltration.	Reduces the risk of insider threats and external attacks that exploit SSH for pivoting within the network.
Service-Specifies Access Rule	Allows specified services (HTTP, HTTPS, FTP) to access the DMZ, tailoring access permissions to the specific requirements of each service while maintaining strict control over what types of interactions are allowed.	Ensures that only necessary communications occur between the internal network and the DMZ, thereby enhancing security by minimizing potential entry points for attackers and reducing the attack surface.
Egress Filtering Rule	Controls what types of data can leave the network. This rule is essential for preventing data loss and ensuring that outgoing traffic conforms to corporate policies and regulatory requirements.	Prevents sensitive data leakage and blocks communication with malicious external entities. It also ensures compliance with data protection regulations.

05 - RECOMMENDATIONS FOR FUTURE IMPROVEMENTS

- **Continuous Security Audits and Monitoring**

Rationale: Critical role of regular security audits in identifying and mitigating vulnerabilities.

Recommendation: Implement a continuous security monitoring program that includes automated tools to regularly scan the network for vulnerabilities. This should be complemented by periodic manual audits to ensure comprehensive coverage.

- **Advanced Threat Detection Technologies**

Rationale: As threats evolve, so must our capabilities to detect and neutralize them.

Recommendation: Invest in advanced threat detection technologies such as machine learning-based solutions that can predict and detect sophisticated cyber threats before they impact the network.

- **Expansion of Security Policies to Include IoT and Mobile Devices**

Rationale: The growing use of IoT and mobile devices introduces new vulnerabilities.

Recommendation: Extend existing security policies to fully cover IoT and mobile devices, ensuring these devices comply with enterprise security standards before they connect to the network.

- **Regular Training and Awareness Programs**

Rationale: Human error remains one of the largest security vulnerabilities.

Recommendation: Implement ongoing security training and awareness programs for all employees to keep security at the forefront of their daily activities and improve their ability to recognize phishing attempts and other social engineering attacks.

08 - PERSONAL AND TECHNICAL REFLECTION

- **Personal reflection:**
 - Challenging yet rewarding experience
 - Improve problem-solving skills
 - Improve teamwork
- **Technical reflection:**
 - Deepened my understanding of how to design and implement security measures in a real-world setting
- **Overall:**
 - Reinforced my interest in cybersecurity and highlighted the continuous need for learning and adapting in this field

09 - CONCLUSION

- **Key achievements:**
 - Robust security enhancement
 - Customized security policies
- **Lessons learned**
 - Importance of regular monitoring
 - Adaptability is key
 - Employee awareness