

**ANALYZING FIREWALL POLICY AND OBJECT INTEGRITY: A GRAPH
DATABASE APPROACH TO MISCONFIGURATION DETECTION AND
PRIORITIZATION**

By

MUHAMMAD YUSUF HUMAR
22351037

MASTER'S DEGREE
in

MASTER OF INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

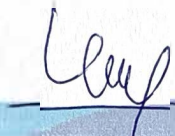


SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

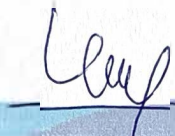
Revision after Thesis Defense on 12 August 2025

STATEMENT BY THE AUTHOR

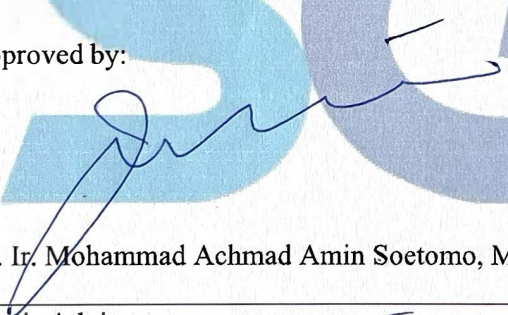
I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.


Muhammad Yusuf Humar

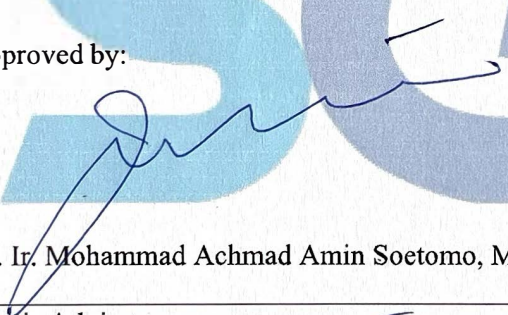
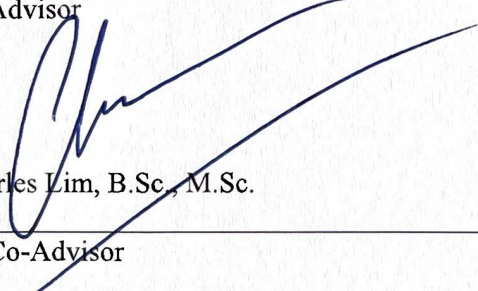
Student


24/08/2025
Date

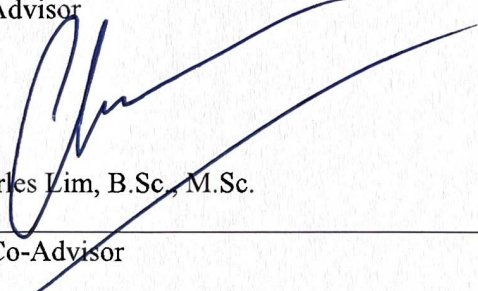
Approved by:


Dr. Ir. Mohammad Achmad Amin Soetomo, M.Sc.

Thesis Advisor


Aug 24th / 25
Date
Dr. Charles Lim, B.Sc., M.Sc.

Thesis Co-Advisor


26/8/25
Date

Dr. Ir. Maulahikmah Galinium, S.Kom., M.Sc.

Dean of Faculty of Engineering and Information Technology

Date

Muhammad Yusuf Humar

ABSTRACT

ANALYZING FIREWALL POLICY AND OBJECT INTEGRITY: A GRAPH DATABASE APPROACH TO MISCONFIGURATION DETECTION AND PRIORITIZATION

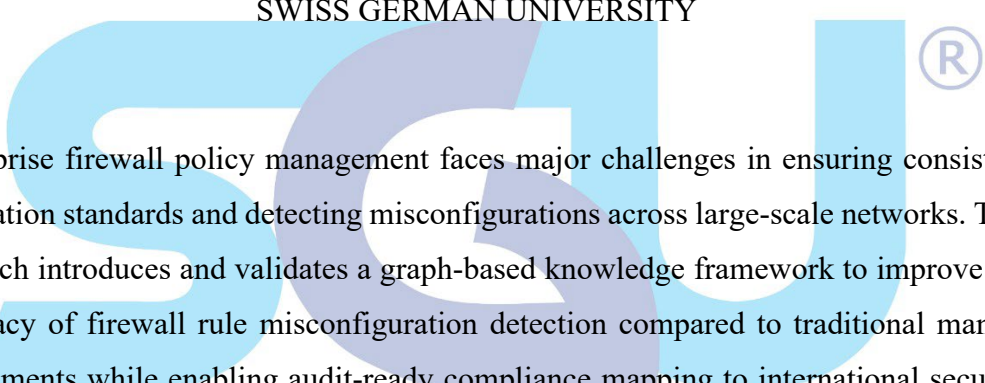
By

Muhammad Yusuf Humar

Dr. Ir. Mohammad Achmad Amin Soetomo, M.Sc., Advisor

Dr. Charles Lim, B.Sc., M.Sc., Co-Advisor

SWISS GERMAN UNIVERSITY

The logo of the Swiss German University (SGU) is a large, stylized 'SGU' in light blue, with a registered trademark symbol (®) to its right. It is positioned behind the abstract text.

Enterprise firewall policy management faces major challenges in ensuring consistent evaluation standards and detecting misconfigurations across large-scale networks. This research introduces and validates a graph-based knowledge framework to improve the accuracy of firewall rule misconfiguration detection compared to traditional manual assessments while enabling audit-ready compliance mapping to international security standards. Using a Design Science Research methodology, the study follows a seven-phase approach: problem identification, data preparation, graph modeling, algorithm execution, scoring, compliance mapping, and validation. The proposed solution incorporates automated detection algorithms addressing five key misconfiguration types: shadow rules, overly permissive access, expired or unused policies, unused objects, and inconsistent object naming. A graph database system processes firewall configuration data via CSV exports, constructs relationship models between policies and network objects, and uses graph traversal to detect rule dependencies and conflicts. Validation combines internal focus group discussions with security professionals, performance benchmarking against prior research, and real-world case study evaluations. Results show the graph-based analysis achieves 85% detection accuracy, identifies 25% more improvement opportunities, and reduces evaluation time by 40%

compared to manual reviews. The compliance mapping component links technical findings to NIST cybersecurity standards, offering structured justification for policy assessments aligned with regulatory audit requirements.

Keywords: Graph Database, Firewall Policy Analysis, Misconfiguration Detection, Policy Anomalies, Cybersecurity Standards



© Copyright 2025
by Muhammad Yusuf Humar
All rights reserved



DEDICATION

I dedicate this work to Allah SWT, to the Prophet Muhammad SAW, to my beloved parents, my brothers, and my sister, who have always given me love and support. I also dedicate it to my team in SXI, whose spirit and cooperation have inspired me, and to my country, Indonesia, which continues to give me purpose and motivation.



ACKNOWLEDGEMENTS

First, I want to thank Allah SWT for all the blessings in my life, for guiding me, and for giving me this opportunity and experience. I also thank the Prophet Muhammad SAW, who always brings hope and guides people in the way of goodness.

Thank you very much to my parents, my brothers, my sister for their praying and all the support during my study at Swiss German University.

A very special thanks goes to someone close to me, who always gave me encouragement, understanding, and patience during the hardest moments of this journey. Your support has meant a lot and helped me stay strong.

I am very thankful to my advisor, Dr. Ir. Mohammad Achmad Amin Soetomo, M.Sc., and my co-advisor, Dr. Ir. Charles Lim BSc., MSc., for their invaluable guidance, insightful advice, and continuous support throughout this research. Their expertise, knowledge and encouragement helped me shape and finish this work.

I would also like to express my gratitude to my colleagues in the SXI team, who shared valuable insights and inspired me with ideas that helped me in developing this research.

Finally, I would like to acknowledge my colleagues and classmates, whose constructive discussions and collaboration gave me many new ideas for this research. And I hope this work contributes meaningfully to the advancement of cybersecurity practices.

TABLE OF CONTENTS

	Page
STATEMENT BY THE AUTHOR.....	2
ABSTRACT.....	3
DEDICATION	6
ACKNOWLEDGEMENTS	7
TABLE OF CONTENTS.....	8
LIST OF FIGURES	10
LIST OF TABLES	11
CHAPTER 1 – INTRODUCTION	13
1.1. Background.....	13
1.2. Research Problem	15
1.3. Research Objective	17
1.4. Research Question	17
1.5. Hypothesis.....	17
1.6. Significance of Study	18
1.7. Scope and Limitation of Study	19
1.8. Thesis Structure	19
CHAPTER 2 – LITERATURE REVIEW	20
2.1. Introduction.....	20
2.2. Terminology Clarification	21
2.3. Regulatory and Threat Landscape of Indonesian Banking	23
2.4. Foundational Concepts in Next-Generation Firewall Management	27
2.5. A Taxonomy of Firewall Policy and Object Misconfigurations.....	29
2.6. Graph Database and Knowledge Graph Technologies	38
2.7. Firewall Object Mapping Fundamentals.....	41
2.8. Methodologies for Automated Firewall Policy Analysis.....	43
2.9. Framework for Compliance Mapping and Scoring.....	49
2.10. Proposed Research Framework Integration	51
2.11. Previous Studies.....	52
2.12. Conclusion: Adopted Methods and Framework	60
CHAPTER 3 – RESEARCH METHODS	62

3.1. Research Design.....	62
3.2. Proposed Research Framework.....	64
3.3. Technology Selection Justification	69
3.4. Research Framework Building Blocks	69
3.5. Research Dataset Description	71
3.6. Data Preparation.....	73
3.7. Graph Modeling	75
3.8. Manual Detection Baseline	81
3.9. Misconfiguration Detection Execution	94
3.10. Prioritization and Compliance Mapping Framework	132
3.11. The Integrated System Architecture	136
3.12. Success Criteria and Evaluation Framework	138
CHAPTER 4 – RESULTS AND DISCUSSIONS.....	140
4.1. System Implementation Overview.....	140
4.2. Data Processing and Cleaning Results.....	141
4.3. Graph Database Schema Implementation.....	143
4.4. Graph Database Creation and Visualization.....	150
4.5. Algorithm Detection Testing Results.....	152
4.6. Analysis Query Capabilities and Performance	163
4.7. Scoring and Prioritization Results	165
4.8. NIST Compliance Mapping Results	166
4.9. Success Criteria Measurement Results	167
4.10. Research Question Analysis	168
CHAPTER 5 – CONCLUSIONS AND RECOMMENDATIONS	171
5.1. Summary of the Research	171
5.2. Contributions of the Study	172
5.3. Limitations and Recommendations for Future Research.....	173
APPENDIX A.....	175
APPENDIX B	178
APPENDIX C	180
APPENDIX D	182
GLOSSARY	184
REFERENCES	185
CURRICULUM VITAE.....	194

LIST OF FIGURES

Figures	Page
Figure 1.1 Top Targeted Industries in Indonesia (2024)	14
Figure 1.2 Fishbone Diagram	16
Figure 2.1 PAN-OS Object Model Hierarchy.....	28
Figure 2.2 Conceptual Schema of the Proposed Firewall Knowledge Graph	47
Figure 3.1 The Design Science Research Framework	63
Figure 3.2 Research Framework	64
Figure 3.3 Finding Shadow Rule using Tasks	82
Figure 3.4 Finding Shadow Rule using API – Front Page.....	83
Figure 3.5 Finding Shadow Rule using API – Count	84
Figure 3.6 Finding Shadow Rule using API – Get Count.....	85
Figure 3.7 Finding Shadow Rule using API – Warning Message	86
Figure 3.8 Finding Shadow Rule using API – Get Shadow Rule.....	87
Figure 3.9 Finding Overly Permissive Access.....	88
Figure 3.10 Finding Expired and Unused Policy.....	89
Figure 3.11 Finding Unused Objects	91
Figure 3.12 Finding Object Naming/Value Mismatch – Address Object.....	92
Figure 3.13 Finding Object Naming/Value Mismatch – Application Object.....	93
Figure 3.14 Finding Object Naming/Value Mismatch – Service Object.....	94
Figure 4.1 Shadow Rule Detection – FPAD Framework Results.....	154
Figure 4.2 Shadow Rule Detection – FOL Knowledge Graph Result.....	155
Figure 4.3 show the result of shadow rule detection using HSVIZ Visualization.....	156
Figure 4.4 Shadow Rule Detection – Classification and Scoring Framework Result.....	158
Figure 4.5 Overly Permissive Access Detection Results.....	159
Figure 4.6 Unused Object Detection Results – Address Objects.....	161
Figure 4.7 Unused Object Detection Results – Service Objects.....	161
Figure 4.8 Unused Object Detection Results – Application Objects.....	162
Figure 4.9 Object Naming/Value Mismatch Detection Results.....	163

LIST OF TABLES

Table	Page
Table 2.1 Graph Database vs Knowledge Graph.....	22
Table 2.2 Policy-Level Misconfiguration Types and Examples.....	31
Table 2.3 Object-Level Misconfiguration Types and Examples	32
Table 2.4 Example of Shadow Rule Misconfiguration.....	33
Table 2.5 Example of Overly Permissive Access Misconfiguration	34
Table 2.6 Example of Expired Policy Misconfiguration	35
Table 2.7 Example of Unused Policy Misconfiguration.....	35
Table 2.8 Example of Unused Object Misconfiguration	36
Table 2.9 Example of Object Naming/Value Mismatch Misconfiguration.....	37
Table 2.10 Research Target Misconfigurations	37
Table 2.11 Graph Database vs Regular Database Comparison	39
Table 2.12 Knowledge Graph Security Applications Framework.....	40
Table 2.13 Object-Policy Relationship Model.....	41
Table 2.14 Comparison of Commercial Policy Management Platforms	44
Table 2.15 Measurement score of misconfiguration attributes by (Park, Park and Kim, 2025)	50
Table 2.16 Critical Review of Previous Studies	53
Table 3.1 Firewall Configuration Dataset Structure	72
Table 3.2 Firewall Knowledge Graph Schema	76
Table 3.3 Misconfiguration Prioritization Matrix.....	133
Table 3.4 NIST SP 800-41 Compliance Mapping	135
Table 3.5 Success Criteria Measurement Framework	138
Table 4.1 Summary of Data	140
Table 4.2 Node Creation Results	151
Table 4.3 Shadow Rule Detection – FPAD Framework Results	153
Table 4.4 Shadow Rule Detection – FOL Knowledge Graph Result	155
Table 4.5 Shadow Rule Detection – HSViz Visualization Result	156
Table 4.6 Shadow Rule Detection – Classification and Scoring Framework Result.....	157
Table 4.7 Overly Permissive Access Detection Results	158
Table 4.8 Unused Object Detection Results	160

Table 4.9 Object Naming/Value Mismatch Detection Results	162
Table 4.10 Misconfiguration Detection Results Summary	163
Table 4.11 Complete Graph Database Query Types and Firewall Management Implications.....	164
Table 4.12 Query Performance Results	164
Table 4.13 Risk Scoring Matrix Application Results	165
Table 4.14 Critical Priority	166
Table 4.15 Medium Priority	166
Table 4.16 Low Priority	166
Table 4.17 NIST SP 800-41 Compliance Mapping Results	167
Table 4.18 Processing Performance.....	168
Table 4.19 Detection Coverage.....	168

