

# **Network Firewall and Access Management System**

**K.D.L.I. Lakmal  
2024**



# **Network Firewall and Access Management System**

**A thesis submitted for the Degree of Master of  
Information Technology**

**K.D.L.I. Lakmal**

**University of Colombo School of Computing  
2024**



# Declaration


<b>Name of the student: K.D.L.I Lakmal</b>
<b>Registration number: 2020/MIT/055</b>
<b>Name of the Degree Programme: Master of Information Technology</b>
<b>Project/Thesis title: Network Firewall and Access Management System</b>

1. The project/thesis is my original work and has not been submitted previously for a degree at this or any other University/Institute. To the best of my knowledge, it does not contain any material published or written by another person, except as acknowledged in the text.
2. I understand what plagiarism is, the various types of plagiarism, how to avoid it, what my resources are, who can help me if I am unsure about a research or plagiarism issue, as well as what the consequences are at University of Colombo School of Computing (UCSC) for plagiarism.
3. I understand that ignorance is not an excuse for plagiarism and that I am responsible for clarifying, asking questions and utilizing all available resources in order to educate myself and prevent myself from plagiarizing.
4. I am also aware of the dangers of using online plagiarism checkers and sites that offer essays for sale. I understand that if I use these resources, I am solely responsible for the consequences of my actions.
5. I assure that any work I submit with my name on it will reflect my own ideas and effort. I will properly cite all material that is not my own.
6. I understand that there is no acceptable excuse for committing plagiarism and that doing so is a violation of the Student Code of Conduct.

<b>Signature of the Student</b>	<b>Date (DD/MM/YYYY)</b>
	29/09/2024

Certified by Supervisor(s)

This is to certify that this project/thesis is based on the work of the above-mentioned student under my/our supervision. The thesis has been prepared according to the format stipulated and is of an acceptable standard.

	<b>Supervisor 1</b>	<b>Supervisor 2</b>	<b>Supervisor 3</b>
<b>Name</b>	Dr. Kasun Karunanayaka		
<b>Signature</b>			
<b>Date</b>	30/09/2024		

## **Abstract**

This document outlines the development and implementation of the web-based Network Firewall and access management system, designed to automate the firewall port open request process, vulnerability assessment request process, Internet access request process and Active Directory password create/reset request process within the IT department of Bank of Ceylon.

When number of requests arises, it leads to misplace of request forms and extra effort should be made to maintain old records. The major issue is when request come up with expiry date, network team becomes responsible for removing the access after expiration date. If document is miss placed it becomes a huge risk. Also, when hard copies of requests forms are maintained, the staff needs to put an extra effort when retrieving the needed information. In vulnerability assessment process each unit and security department has to keep files separately that has same details. Due to the manual system, there are frequent data entry errors, data duplication and misprocessing of data. The staff need to put in extra work to retain team-specific information and them accordingly to obtain a comprehensive picture of the status of all requests. Not only that, but also the higher management is unable to view the status of the vulnerability fixing since referring to excel sheets of each and every division is time consuming. Web-based Network Firewall and access management system was developed as a solution to convert current paper based manual process to digital platform based process.

The designed system's main aim is to monitor all the Firewall, VA, Internet and password create/reset requests and identify the unnecessary bottle necks. The system was developed as a fully web-based application with MySQL as the database and PHP scripting language for application. Users can access the application via the bank's internal network with any browser of their choice. It is projected to improve employee productivity in the IT sector as well as information accuracy and efficiency. Testing and the evaluation done by the selected users from each unit in IT department including higher management. The developed system demonstrated to users and feedback. Positive user feedback indicates that the system satisfies the specified need and is an improvement over the existing manual procedure.

## **Acknowledgement**

First and foremost, I would like to express my sincere gratitude to my project supervisor Mr. Kasun Karunanayaka for his exceptional guidance and unwavering support throughout the duration of my project. His friendly demeanor and encouragement have played a crucial role in motivating me to stay focused and committed to meeting deadlines. His dedication to reviewing our work meticulously and providing constructive feedback has not only ensured the success of my tasks but has also helped me grow both personally and professionally. His willingness to share his expertise and insights has been invaluable, and I am truly thankful for his mentorship.

I also want to express my gratitude to the employees of the Bank of Ceylon's Internet Security department, Technical department, and Network department and to Mr. S.M Rinos, Chief Manager of IT Delivery channels, for their invaluable assistance during the system's conception, development, and evaluation phases. Their assistance cleared the path for a well-designed system.

Last but not least, I would want to express my gratitude to my parents, my beloved wife, and my close friends for their understanding, encouragement, and support in helping me to successfully finish this project.

# Table of Contents

<b>Declaration.....</b>	<b>iii</b>
<b>Abstract.....</b>	<b>iv</b>
<b>Acknowledgement.....</b>	<b>v</b>
<b>List of Figures.....</b>	<b>ix</b>
<b>List of Tables .....</b>	<b>xi</b>
<b>List of Abbreviations .....</b>	<b>xii</b>
<b>Chapter 1 – Introduction .....</b>	<b>13</b>
1.1    Project Overview.....	13
1.2    Motivation.....	14
1.3    Objectives.....	16
1.4    Background of the study .....	17
1.5    Scope of the study .....	19
1.5.1.    Administrative Module.....	19
1.5.2.    Firewall Port Access Module .....	19
1.5.3.    Password Reset Module .....	20
1.5.4.    Vulnerability Management Module.....	20
1.5.5.    Request tracking and monitoring Module .....	20
1.5.6.    Reporting module .....	20
1.6    Structure of the dissertation.....	21
<b>Chapter 2 – Background .....</b>	<b>23</b>
2.1    Introduction .....	23
2.2    Requirement Analysis .....	23
2.2.1    Main requirement .....	24
2.2.2    Sub Requirements.....	24
2.2.3    Functional Requirements.....	25
2.2.4    Non-Functional Requirements.....	25
2.3    Review of Similar Systems .....	27
2.3.1    ONTASK.....	27
2.3.2    LEGITO.....	28

2.3.3	KISSFLOW .....	28
2.4	Related Technologies .....	30
2.4.1	Front End Development .....	30
2.4.2	CodeIgniter 4 Framework.....	31
2.4.3	Database Management.....	31
2.4.4	Related Design Strategies.....	31
<b>Chapter 3 – Design Architecture .....</b>		<b>33</b>
3.1	Introduction .....	33
3.2	System Architecture .....	33
3.3	UML Diagrams .....	36
3.3.1	Use case Diagrams .....	36
3.3.2	Use case narrations .....	41
3.3.3	Sequence Diagrams .....	46
3.3.4	Class Diagram .....	49
<b>Chapter 4 - Implementation Details.....</b>		<b>50</b>
4.1	Architecture of Implementation .....	50
4.2	Query Builder Class .....	53
4.3	Look and Feel of the web application .....	55
<b>Chapter 5 – Testing and Evaluation.....</b>		<b>56</b>
5.1	Introduction .....	56
5.2	System Testing .....	56
5.2.1	Test Cases.....	57
5.2.2	Testing Status .....	60
5.3	System Evaluation.....	60
5.4	Analysis of the Results.....	63
<b>Chapter 6 – Conclusion .....</b>		<b>69</b>
6.1	Future Work .....	70
<b>List of References .....</b>		<b>71</b>
<b>Appendix A – MIS Reports.....</b>		<b>73</b>
<b>Appendix B – Test Plan .....</b>		<b>79</b>

<b>Appendix C – User Manual.....</b>	<b>83</b>
--------------------------------------	-----------



# List of Figures

FIGURE 1.1: FLOWCHART OF THE TRADITIONAL SYSTEM .....	17
FIGURE 3.1: SYSTEM ARCHITECTURE DIAGRAM.....	33
FIGURE 3.2: CODEIGNITER ARCHITECTURE .....	35
FIGURE 3.3: USE CASE DIAGRAM FOR ADMINISTRATIVE MODULE .....	36
FIGURE 3.4: USE CASE DIAGRAM FOR FIREWALL PORT ACCESS MODULE.....	37
FIGURE 3.5: USE CASE DIAGRAM FOR PASSWORD RESET MODULE .....	38
FIGURE 3.6: USE CASE DIAGRAM FOR VULNERABILITY MANAGEMENT MODULE .....	39
FIGURE 3.7: USE CASE DIAGRAM FOR REPORTING MODULE.....	40
FIGURE 3.8: SEQUENCE DIAGRAM FOR LOGIN .....	46
FIGURE 3.9: SEQUENCE DIAGRAM FOR CREATE NEW USER PROFILE.....	47
FIGURE 3.10: SEQUENCE DIAGRAM FOR CREATE NEW FIREWALL REQUEST .....	48
FIGURE 3.11: CLASS DIAGRAM OF THE WEB APPLICATION.....	49
FIGURE 4.1: FOLDER STRUCTURE .....	50
FIGURE 4.2: ROUTING SYNTAX.....	51
FIGURE 4.3: CONTENT OF DATABASE.PHP .....	52
FIGURE 4.4: INSERT QUERY IN QUERY BUILDER.....	54
FIGURE 4.5: SAMPLE WEB PAGE .....	55
FIGURE 5.1: EVALUATION FORM .....	62
FIGURE 5.2: GRAPH FOR CATEGORY WISE RATING .....	64
FIGURE 5.3: RATING ON LOOK & FEEL OF THE WEBSITE .....	65
FIGURE 5.4: RATING ON PERFORMANCE OF THE APPLICATION .....	66
FIGURE 5.5: RATING ON SYSTEM USEFULNESS .....	66
FIGURE 5.6: RATING ON SYSTEM INFORMATION ACCURACY .....	67
FIGURE 5.7: RATING ON SYSTEM SECURITY .....	67
FIGURE 5.8: RATING ON SYSTEM AVAILABILITY .....	68
FIGURE 5.9: SUMMARY OF OVERALL USER EXPERIENCE .....	68
FIGURE A.1: USER LIST .....	74
FIGURE A.2: USER LIST INACTIVE .....	74
FIGURE A.3: FIREWALL ACCESS DETAIL REPORT .....	75
FIGURE A.4: INTERNET ACCESS EXPIRATION REPORT .....	76
FIGURE A.5: VULNERABILITY ASSESSMENT REQUEST REPORT.....	77
FIGURE A.6: AD PASSWORD MAINTENANCE DETAIL REPORT .....	78
FIGURE C.7: USER LOGIN.....	83
FIGURE C.8: USER DASHBOARD .....	84

FIGURE C.9: FIREWALL PORT OPEN REQUEST FUNCTION .....	85
FIGURE C.10: SUCCESSFUL REQUEST .....	86
FIGURE C.11: VA REQUEST FUNCTION .....	87
FIGURE C.12: INTERNET REQUEST FUNCTION .....	88
FIGURE C.13: PASSWORD CREATE/RESET FUNCTION .....	89
FIGURE C.14: UNIT MANAGER APPROVAL .....	90
FIGURE C.15: MORE DETAILS OF PENDING APPROVALS .....	91
FIGURE C.16: PANEL FOR PENDING INTERNET REQUEST FOR APPROVAL .....	92
FIGURE C.17: PANEL FOR PENDING VA REQUEST FOR APPROVAL.....	93
FIGURE C.18: PANEL FOR PENDING PASSWORD REQUEST FOR APPROVAL .....	93
FIGURE C.19: AUTHORIZATION FUNCTION .....	94
FIGURE C.20: MORE DETAILS OF SELECTED RECORD OF A PENDING APPROVAL .....	95
FIGURE C.21: EXECUTE FUNCTION .....	96
FIGURE C.22: PENDING INTERNET REQUESTS .....	97
FIGURE C.23 PENDING VA REQUESTS.....	97
FIGURE C.24: PENDING PASSWORD/RESET.....	98
FIGURE C.25: ADMINISTRATIVE FUNCTION.....	99
FIGURE C.26: USER MODULE SUCCESSFUL NOTIFICATION .....	100
FIGURE C.27: USER LIST .....	100
FIGURE C.28: ROLE GROUP FUNCTION .....	101
FIGURE C.29: EDIT USER ROLE .....	102
FIGURE C.30: ROLE MODULE ASSIGNMENT .....	103

# List of Tables

TABLE 1: FEATURE COMPARISON WITH SIMILAR SYSTEMS (SOURCEFORGE, 2023). .....	29
TABLE 2: USE CASE NARRATION FOR LOGIN.....	41
TABLE 3: USE CASE NARRATION FOR CREATE NEW USER PROFILE .....	42
TABLE 4: USE CASE NARRATION FOR CREATE NEW DEMAND MANAGER REQUEST .....	43
TABLE 5: USE CASE NARRATION FOR PASSWORD RESET .....	44
TABLE 6: USE CASE NARRATION FOR VULNERABILITY ASSESSMENT REQUEST .....	45
TABLE 7: TEST CASES FOR LOGIN.....	58
TABLE 8: TEST CASES FOR USER REGISTRATION .....	59
TABLE 9: STATUS OF TEST CASES.....	60
TABLE 10: EVALUATION RESULTS .....	63
TABLE B.11:VA REQUEST TEST CASE .....	79
TABLE B.12: TEST CASE FOR FIREWALL PORT OPEN REQUEST .....	80
TABLE B.13: TEST CASE FOR USER ROLE .....	81
TABLE B.14: STATUS OF TEST CASES.....	82

## List of Abbreviations

AD	Active Directory
BOC	Bank of Ceylon
LDAP	Lightweight Directory Access Protocol
MVC	Model-View-Control
QA	Quality Assurance
UAT	User Acceptance Testing
VA	Vulnerability Assessment
PF	Provident Fund
IT	Information Technology
ATM	Automated Teller Machine
UI	User Interface
DR	Disaster Recovery
CSS	Cascading Style Sheets
DB	Database
PHP	Hypertext Preprocessor
CDM	Cash Deposit Machine

# Chapter 1 – Introduction

## 1.1 Project Overview

Bank of Ceylon (Bank of Ceylon., 2017) is a significant state-owned commercial bank in Sri Lanka which has a network of 649 branches, owning more than 735 Automated teller machines (ATMs), 159 cash deposit machines (CDM) and 544 ECRM island wide.(Sunstein, 2019) Due to the sensitivity of the information handled and the high value of the assets dealt with, security is one of the main concerns of a bank. Though Internet provides many services to the public, to banking industry it could be a double-sided sword. The reason is that it provides vast services to the world while allowing unlimited access to the banking systems. Therefore, managing Internet Security is a major aspect in a bank. The Internet Security team in a bank involves in managing access to bank systems, assessing vulnerability in servers, configuring security in devices, as well as monitoring the devices and applications to identify any security threats.

According to old manual process IT security team and the technical department separately maintain the Physical documents to keep record. The major issue is when request come up with expire date, Network team will responsible for remove the access when expire date reach. If document is miss placed it became a huge risk. If the management want pass record there is no way to get the needed data quickly. Staff need to search needed data in physical files. In vulnerability assessment process each unit and security department has to keep files separately that has same details (Radostin Dimov et al., 2021). Due to the manual method, there are frequent data entry errors, and the staff need to put in extra work to retain team-specific information and combine it as necessary to obtain a comprehensive picture of the status of all requests. Not only that, but also the higher management is unable to view the status of the vulnerability fixing since referring to excel sheets of each division consumes more time.

The main objective of this project is to provide a solution to automate the manual form handling process within the IT section. The proposed solution will be effective to the whole BOC branch network. This solution can reduce the paper work allowing the management to get live status of the firewall requests sent by IT staff(Muhammad Abedin et al., 2010). This will allow to identify the bottlenecks of the existing process. The old system unable to facilitate top management to track

the request. Using new solution top management able to monitor the status any time to avoid unnecessary delays. This software solutions helps to improve efficiency, accuracy, and productivity of the firewall request process by replacing time-consuming and error-prone manual processes with automated workflows, the organization seeks to enhance overall performance, reduce costs, and improve the quality of its services. Not only that, but also the IT Security team receives nearly 20 forms per day and it leads to huge paper waste since copies are maintained in different sections. Not only that but also, a considerable amount of time is wasted during this approval process due to maintenance of hard copies. At present, lack of paper material is one of the major issues in Sri Lanka, therefore wasting several papers to gain access to one system would be huge cost to the bank. Reporting function of Web based system for Firewall and Access Management give quick access to old records. Security and network team will be able to handle the requests sent to them smoothly and efficiently.

## **1.2 Motivation**

The major issues identified by analyzing the existing manual process of the IT Security team is shown given below.

- Firewall request forms submitted as a paper-based form where it contains all details related to ports that needs to be opened. The paper contains the sensitive data like server IP addresses and ports which will be opened in the future. Without using electronic media, it will raise the security concern that a misplaced document can get into the hands of the unauthorized person.
- The printed firewall request forms will be signed by the responsible chief manager and handed over to the internet security team. Then they put the comment and keep the original document with them and copy of the document is given to the network team. So, both team have to keep physical storage space to maintain the documents. When implementing new systems and new branches are opened, it will lead to increases the number of documents.

It will be time consuming and require unnecessary human resources. Due to paper work it has huge paper cost.

- Sometimes it will delay the requests to grant permission. In manual systems, there is no way to identify the bottleneck. If we use electronic media, we can use the reports and the monitor the flow of authentication part to identify the bottle neck. Therefore, higher management can monitor the flow and involve in solving unnecessary delays in form handling.
- The Network Operations team configure two types of system access namely permanent and temporary. It is their responsibility to remove access from the users on the expiry date of temporary allowed access. At present, these forms are checked manually by the network team to remove access from the users. Checking these forms daily is not an easy task and it could lead to human errors. Both the Network Team and the IT Security team put great effort in handling these forms and it has become an additional work load to their daily tasks.
- In the process of server vulnerability fixing, each unit must maintain the excel sheet to maintain the vulnerability status of every server. Internet Security Team should maintain the unit wise excel sheet so that, every server owner and the security team member must put an extra effort on maintaining the details rather than the maintain physical request forms. Even though security team maintain the shared file in shared location, it will not allow to modify the files at the same time.
- Authorized requests are applied by the network team. In this final phase, communications between the requester and the network team will be handled only through phone calls. It may delay the projects related to ports that needs to be opened.
- When historical data is needed it takes more time to search information since all files exist as physical documents. Sometimes is difficult to find data due to this reason and it clearly shows the need for an automated system to handle the forms.
- When generating reports for the corporate management on vulnerability status, it will be required to combine each of all unit wise excel sheets and maintained by different units.

So this process will be time consuming and there may be human errors in manual data entry that can lead to data inconsistencies, invalid entries, and compliance issues(Indeed, 2023).

- Higher management is unable to view the status of the vulnerability fixing since referring to excel sheets of each division consumes more time.

Because of the above difficulties and concerns, there is a need of developing a software to automate the manual firewall request and vulnerability fixing process. By implementing web-based Network Firewall and Access Management System, it is expected to increase the productivity by reducing the time taken to handle a firewall request, data accuracy, efficiency, security of information by given access to authorized personnel. Also, it will help to reduce the usage of papers and implement green concept within the office premise. Data in electronic media will help to generate different kind of reports and allow higher management to monitor the firewall request handling and identify the bottlenecks of the existing process.

### **1.3 Objectives**

The primary goal of this project is to create a web-based system for Firewall and Access Management which could be used to automate the existing manual procedure. This system will help the Internet Security and the Network teams to overcome the human errors and limitations in access maintenance and vulnerability fixing (Radostin Dimov et al., 2021).

Given below are the key objectives of the proposed Firewall and Access Management System.

- Register and maintain the basic information of the division of the IT department.
- Register IT Staff and assigning them to divisions.
- Handle firewall port opening requests managed by different managerial approval levels.
- Handle password reset requests managed by different managerial approval levels.
- Handle vulnerability status of servers managed by each division in IT Department.
- Provide overall visibility of the request status to the higher management of the IT department and all other units.



- Determine the Bottlenecks in the workflow by tracking the time taken to complete certain tasks.
- Generate email notification to network team to remove temporary access when expiry date is reached.

## 1.4 Background of the study

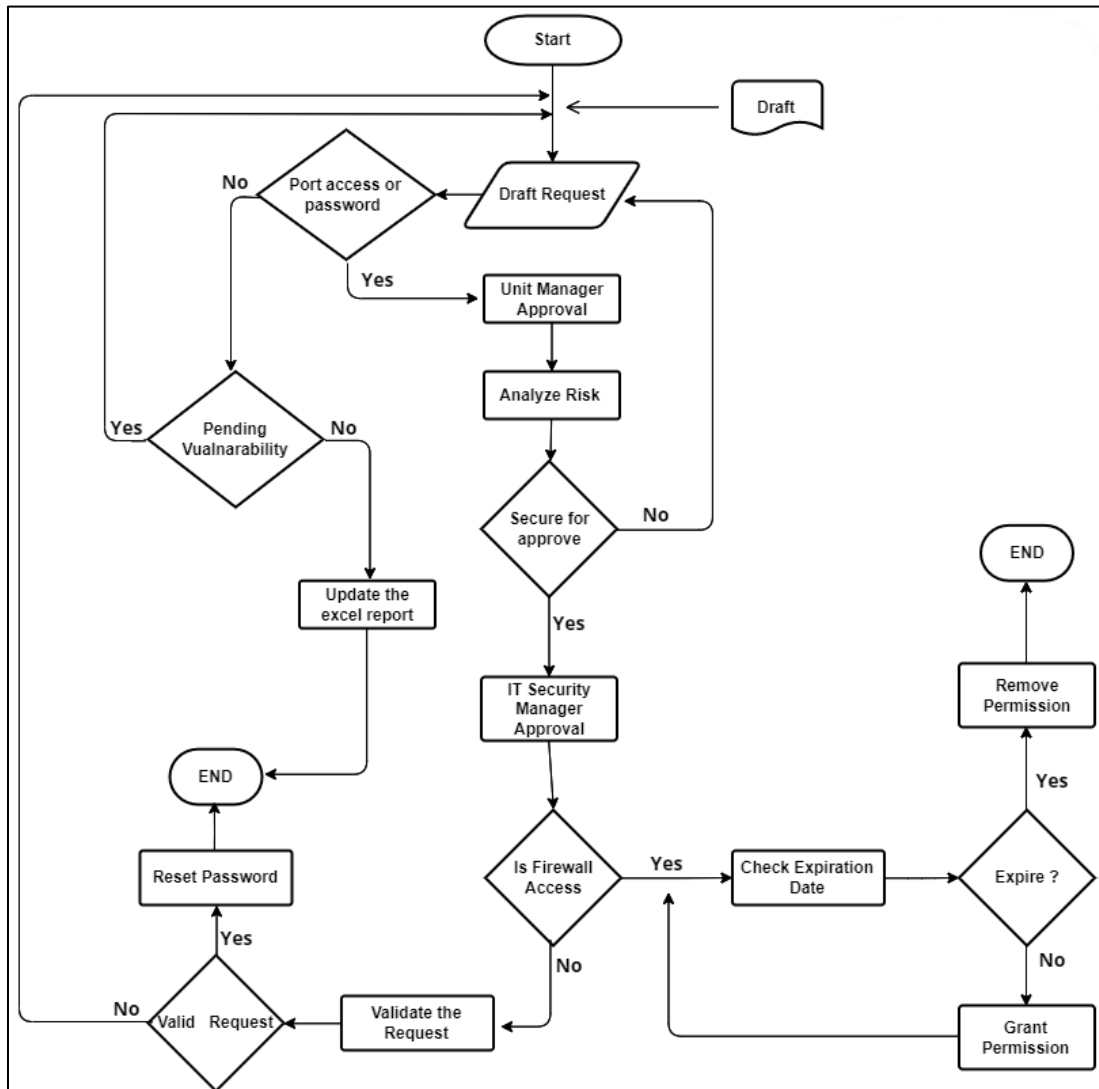


Figure 1.1: Flowchart of the Traditional System

At BOC, requests for IT firewall port opening and resetting passwords are handled manually. Each unit requests different types of access to the systems and devices which require approvals of the higher management. The IT system users must print access control forms and the completed forms are then provided to the relevant senior managers for the confirmation. The confirmed form is then transferred to the chief manager for the higher management approval and then be forwarded to the IT Security team for review. When implementing new projects multiple ports will be opened for new servers and these servers need to be scanned to identify vulnerabilities.

The identified vulnerabilities need to be fixed and rescanned until all the issues are fixed. Each time these firewall request forms are submitted to the IT Security team, it is the responsibility of the IT Security team to check the ports, source and destination IP addresses to analyze the risk associated with it. The reviewed form will then be forwarded to the Chief Manager of IT Security division for the approval if the risk could be managed. In case, if there is a high risk or any modifications to the form is needed, it would be returned to the relevant division. The approved form is then sent to the Network Operations Center for the configuration. Both the IT Security and the Network Team maintain separate copies of the Access Forms for future reference and audit purposes. Finally, the request will be fulfilled by the network team and will be informed to the relevant unit. Not only handling these requests but also removing access from the expired access must be handled properly by the Network Team.

Currently, password reset process is also handled manually. The user must inform the password request by email from technical department. It is responsibility of technical department to check and validate the user and reset the password. The vulnerability assessments are conducted on the servers quarterly to check the risk status of the servers. When implementing new systems new servers required to conduct the vulnerability scan and fix all vulnerability issues that are detected in the scan. Relevant team requests the scan by an email and IT security team will generate the vulnerability assessment report. These reports are maintained in Excel sheets which are distributed among the divisions to fix the vulnerabilities. After the issues are fixed by the relevant teams, they must update the excel sheet with the vulnerability status. IT security team maintains separate excel sheets for the teams to maintain the vulnerability status of each unit. Finally, they generate a report

for corporate management on vulnerability status and will be analyzed to make decisions on implementing rules and regulations.

## **1.5 Scope of the study**

The developed system consists of five major modules.

### **1.5.1. Administrative Module**

- User Profile Management:
  - Users with administrative privileges can add/edit and disable the users.
- User Role management
  - Define the user roles with privileges and assign it to the registered users. The system will be able to control user access to each function.
- Manage Units in the IT department
  - Users with Administrative privileges can Add/Edit and disable the department.

### **1.5.2. Firewall Port Access Module**

- Initiate a port access request form by a requester.
- Check by senior manager and approved by the relevant unit chief manager. Submit the form to the security team.
- Conduct a risk analysis by the security team and submit to the chief manager of security team with comments.
- Approved requests submit to the network team. Rejected requests will be returned to the requester through his higher management.
- Network team attend to the task and grant permission to the requester.
- Network team remove temporary access when the expired date is reached by checking the received email notification.

### **1.5.3. Password Reset Module**

- Initiate password reset request form by a requester.
- Check by senior manager and approved by the unit chief manager. Submit the form to the technical team.
- Network team attend to the task.

### **1.5.4. Vulnerability Management Module**

- Each team send the Vulnerability Assessment (VA) scan request.
- Security team conduct the VA scan and generate the report.
- The generated report will be uploaded to the system and will be visible to the relevant division.
- The unit can download the report and fix the vulnerabilities.

### **1.5.5. Request tracking and monitoring Module**

- Each unit can track their request to check whether it is processed.
- Higher management would be able to use the dashboard to identify the bottleneck and speed-up the process.
- Chief Manager of each unit has authority in their dashboard to monitor the tasks daily.

### **1.5.6. Reporting module**

- Generate user report by Administrator.
- Firewall port access report, rejected request report generated by each division in IT department.

- Pending requests (password reset, VA scan, and firewall port access) report to identify bottleneck.
- Daily Access expiration report generated by Network Team.

## 1.6 Structure of the dissertation

The remaining chapters of the dissertation are organized as follows;

First chapter mainly focuses on the introduction of the system which has been developed. It briefly mentions the problems of the current manual system, the solutions and the scope of the developed system. The second chapter provides an overview of the system's background and reviews relevant literature on similar systems and technologies. It examines the requirements analysis along with various technologies and design strategies employed in the project's development. In the third chapter, the focus shifts to requirement analysis and solution design, featuring comprehensive UML diagrams including the Deployment, Component, Class, and Sequence diagrams, as well as database design represented through ER diagrams. Chapter five evaluates the system, assessing whether the project objectives were met. It details the methods used for data analysis, addresses any shortcomings in the final product, and outlines the steps taken to enhance functionality. This chapter also offers recommendations for future developments and discusses lessons learned throughout the process. Finally, the sixth chapter concludes the project by summarizing the limitations of the techniques used and proposing potential solutions, while also highlighting the benefits that the project brings to the bank.

- Chapter 1 – Introduction

This chapter provides a vivid introduction about this project. It includes the project overview, motivation, objectives, and background of the project and the project scope of the developed system.

- Chapter 2 – Background

This chapter describes the background study of the existing system and comparison between the developed system and similar systems in the market. It also includes the availability of technologies and the justification of selected technologies. This chapter contains a full description about the requirement analysis of the developed system and the different design strategies used in developing the system.

- Chapter 3 – Methodology

This chapter includes all the system diagrams used when developing the system. For example, UML Diagram (Lucidchart, 2023), ER diagram(Ravikiran A S, 2023), EER diagram, Class diagrams(Nishadha, 2023), Component diagrams as well as the system flow diagrams. The wireframes of the developed system used for UI designing would also be included in this section of the dissertation. Apart from that, it also includes how the system is developed and what testing strategies are used to test the system.

- Chapter 4 – Evaluation

Chapter 4 describes the results and the observations of the developed and it analyzes whether the project objectives are fulfilled successfully. This chapter discusses what analyzing tools are used and justification of the used tools. It contains a critical analysis of the advantages and the disadvantages of the proposed system and how it could be improved further to meet the expectations of the organization.

- Chapter 5 – Conclusion

This chapter contains a discussion of the developed system highlighting the limitations and future improvements that could be used to overcome the limitations. It describes the benefits of developing the project to the Bank.

## Chapter 2 – Background

### 2.1 Introduction

This chapter briefly explains the analysis of the requirements of the proposed system and provides the reviews on existing systems that are like the proposed system. Technologies and functionalities of similar systems have been mainly focused when comparing new systems with other similar systems. These technologies have been discussed in detail and justification of the selected technologies have been provided in this section.

### 2.2 Requirement Analysis

After conducting formal discussions with all the IT staff that participate in the firewall port open process, password reset process and the vulnerability assessment process, the gathered requirements analyzed. Based on the discussions, the requirements are broken down into distinct modules, such as:

- **Firewall Management:** Focused on opening and closing ports.
- **Password Management:** Covering the processes for password resets and policy enforcement.
- **Vulnerability Assessment:** Addressing the identification and remediation of security vulnerabilities.

Each module is translated into use cases, which detail interactions between users and the system. This helps clarify the functionality and user scenarios, guiding the development process. To effectively prioritize the requirements identified during analysis, consider the criteria such as Business Impact, User Needs, Feasibility, Risk Mitigation and Dependencies. During the requirement analysis, several potential difficulties may have emerged, including:

- **Complexity of Processes:** Existing processes might be cumbersome, making it challenging to streamline workflows.

- **User Resistance:** There may be resistance to change from staff accustomed to current processes.
- **Integration Issues:** New systems must integrate seamlessly with existing tools and platforms, posing a potential challenge.
- **Scalability:** Ensuring that the new system can handle future growth in users or functionalities is essential.

Class diagrams were designed to identify the whole process and the responsible roles in the new system. These diagrams are explained in detail in the next chapter.

Given below are the overall requirement by teams that involve with the firewall management process, vulnerability assessment process and the password reset process.

### **2.2.1 Main requirement**

- Automation of the existing firewall request authentication process, vulnerability assessment process and the password reset process.

### **2.2.2 Sub Requirements**

- Increase productivity, Data accuracy, efficiency, and the speedup firewall port authentication process.
- Increase data security.
- Reduce paper work and implement green concept within office premise.
- Facilitating management to view progress of firewall request and track the request.
- Facilitate management to view vulnerability status and the progress.
- Reduce unnecessary human resources.
- Facilitate higher management to track the whole process and identify the bottle necks.
- Reduce unnecessary printing cost and the paper cost.



There are two types of requirements. Those are Functional requirements and non- functional requirements. In functional requirements the terms of specific functions, services, or features system are described. It also describes the behavior of the system and its interaction with users. Non-Functional requirements describe the overall behavior, performance, hardware, and software requirements while developing, implementing, and maintaining the system which would help to deliver better user experience from the system.

### **2.2.3 Functional Requirements**

- User registration: The system should allow users to create an account with a unique username and a password. Proposed system must facilitate to manage users with role groups, managing user profiles and managing unit with department in administrative module.
- Search functionality: The system should provide a search feature to allow users to search for specific items or information.
- Authenticate request: The new system must allow users to authenticate and view details of request using different user levels. Higher management will approve the request sent by the different units.
- Reporting: The system should generate daily, weekly, and monthly reports based on user activities.

### **2.2.4 Non-Functional Requirements**

Given below are the non-functional requirements of the proposed Network Firewall and Access Management system (Guru99, 2023).

- Usability – Since the proposed Network Firewall and Access Management system would be accessed by all the staff in the IT department to submit firewall and password reset

requests, the system must be easily accessible and easy to use. It should contain clear functions with directions on how to use them.

- Performance – The proposed system would be used by the higher management to identify bottlenecks and the generated reports would be used for decision making process. Therefore, the system performance is a critical matter since the higher management work to a tight schedule. Also, system performance with minimum delays and failures would save the time of the IT security team, Network Team, and technical team. When developing this application, the consideration of speed, response time, throughput, scalability, and capacity is very important to have better performance. Since the application would be implemented on premise, the bank could extend the resources to increase its performance.
- Security – The proposed system would contain very sensitive data such as server details, vulnerabilities of live servers and open ports with time. Loss or theft of this sensitive data could cause a huge damage to the bank. By considering these facts the proposed system would be implemented on-premises which would completely restrict from outsiders other than authorized persons. Cloud-based solutions are more vulnerable to prying eyes and third parties. On-premises storage might be the best choice for businesses that deal with sensitive data, such as those in the financial sector. Given below are some key points to be considered when securing the application.
  - Ability to modify the access permission for the system's data would only be granted to system's data administrator.
  - All system data must be backed up weekly, and copies of the backup must be maintained in multiple locations.
  - Unauthorized access to the system is restricted.
  - Protect the system's integrity from unintentional or deliberate destruction.
- Maintainability – Proposed system is an internal development. Source code and system will be maintained on-premises. Therefore, it would be easier to maintain the system with less effort and cost. Also, this system would be designed using Model-View-Controller architecture which would enhance the maintainability of the system. Not only that, but also

the system administrators can easily engage in system upgrades and database maintenance since both the application and the database would be hosted on premise.

## **2.3 Review of Similar Systems**

### **2.3.1 ONTASK**

ONTASK(Cision, 2023) by Accusoft is a cloud-based workflow automation and document management solution designed for business of all sizes. It allows users to manage tasks inside their business, automate document procedures, and develop unique workflows. Main Features of ONTASK (OnTask, 2023) are listed below. ONTASK (Accusoft Corporation, 2023) can be used in various industries such as healthcare, education, legal, finance and more.

- Workflow Automation
- Fillable Forms
- Digital Signatures
- Intuitive Dashboard

Although ONTASK(ONTASK, 2023) fulfils the majority of the system's standards, there are few restrictions must be taken care of. ONTASK is a cloud-based solution. As a state-owned bank, it is required to abide by government financial standards, and the product must be assessed through a tendering process. Because of security purpose it's not encourages to store data in cloud. ONTASK(ONTASK, 2016) does not have module to manage users with user roles and manage departments. It Generate emails manually. ONTASK has user limitation, they offer unlimited users for enterprise edition.

### **2.3.2 LEGITO**

Legito (Legito, 2023b) is a cloud-based workflow management technology that aids companies in automating the generation of documents and contracts. Users can easily create, edit, store, and distribute documents and contracts because to its streamlined and straightforward document management features. Legito (Legito, 2023a) is rich workflow tool to power efficiency. Below are the key features of the LEGITO (Legito, 2023c).

- Archiving & Retention
- Change management
- Electronic Signature
- Compliance Management
- Version Control

400K users globally use this tool to create, perform, collaborate, and execute their work. LEGITO (Legito, 2023d) is actively using 59 technologies and including service like Google Analytics, jQuery, and HTML5. This platform mainly designs for departments like Human Resources, Legal, Operations, procurement, and sales. The template editor, custom fields in document records and external sharing is some of popular features.(Software Advice, 2023a) LEGITO do not have automated email system. But manually system can send the email. Although, LEGITO has more many feature its cost is very high. As a state-owned bank, BOC must align with government financial laws. Therefore, product must be evaluated through a competitive bidding procedure, and as a result LEGITO would not be suitable for Bank of Ceylon.

### **2.3.3 KISSFLOW**

OrangeScape Technologies provides KISSFLOW (kissflow, 2023a), a cloud-based form automation system. To assist businesses in automating their workflows, tasks, and procedures. KISSFLOW(Software Advice, 2023b) provides a cloud-based workflow automation platform. By automating tedious and time-consuming procedures, it is a simple and user-friendly platform that

enables organizations to optimize their operations and increase their efficiency. Given below are the main key features of KISSFLOW.

- Dynamic task assignment
- SLAs, deadlines, and escalations
- Drag and drop forms
- Access control
- Reports and Analytics

KISSFLOW (kissflow, 2023b) is a very user-friendly tool which makes the users easy to handle their organizational processes. Due to its cloud-based architecture and the high price in purchasing the application for users, KISSFLOW could not be used in the Bank of Ceylon to perform their desired tasks.

The above scenarios show that Bank of Ceylon needs a system which could be implemented on premise with the features of workflow management, form handling, notifications, and reports generation. Therefore, the proposed system ideally meets all the requirements of the bank.

<b>Features</b>	<b>ONTASK</b>	<b>LEGITO</b>	<b>KISSFLOW</b>	<b>System in Peoples Bank</b>	<b>Proposed Application</b>
User Logging	√	√	√	√	√
User Role management	X	√	√	√	√
On premise	X	X	X	√	√
No charge (monthly or annual charge)	X	X	X	√	√
Auto generated e-mail	X	X	√	X	√
Customize Reporting	X	X	√	√	√
On-Site Support	X	X	X	√	√
Free Database Capacity	√	X	X	√	√

*Table 1: Feature comparison with similar systems (SOURCEFORGE, 2023).*

### **2.3.4 Related Technologies**

Due to rapid development in technology, banks should adapt their existing procedures to align with the new trends. To implement new technologies the banks, need to allow Internet and firewall access to the users. Due to this reason, the IT Security team of the bank face many challenges in managing the risk. Many companies use different strategies to maintain their workflow management and to handle their internal forms. Given below are the tools and technologies used for the development of this system.

### **2.3.5 Front End Development**

This is web-based solution and main purpose is monitoring the process and generate the reports. It is used by different teams and it contain the sensitive data. One of major objective is speedup the process. So front end should have the ability to show data to authorize persons only. Responsiveness and performance are two important factors that should be able to view pages without any delay. This system is used by higher management to get decisions. So, the content should be accurate. In this proposed system mainly use HTML, CSS, and JavaScript.

#### *2.3.5.1 HTML (Hypertext Markup Language)*

It is the standard markup language for creating web pages and applications. It is device independent and platform independent language. HTML is highly compatible with other web technologies and languages. It is easily integrated with CSS and JavaScript. So, for the proposed system it chooses HTML.

#### *2.3.5.2 CSS (Cascading Style Sheets)*

Allow to separate of style and content. CSS is essential for creating responsive web designs that adapt to different screen sizes and devices. It supported by all modern web browsers.

#### 2.3.5.3 *JavaScript*

JavaScript is a high-level programming language developing dynamic and interactive web applications. It supported by all major web browsers. It has popular libraries like jQuery, React and Angular.

### **2.3.6 CodeIgniter 4 Framework**

CodeIgniter 4 framework is used to together with above-described front-end languages. CodeIgniter is an open-source PHP web application framework that follows the Model-View-Controller (MVC) architectural pattern. It is facilitate the features like sending emails, file uploading and session management.(Cynotex, 2020) It is a modern, fast, lightweight, PHP MVC framework that allows you to build secure applications quickly and easily(Udemy, 2023).

### **2.3.7 Database Management**

It is relational database management system develop by oracle that powerful and secure data storage system. It is associate with online applications or web services. MySQL runs on different operating system platforms like Unix-based, Mac OS and Windows. The primary factor differentiating relational databases from other digital storage lies in how data is organized at a high level. It contains records in separate, multiple, collections of semi- or unstructured documents. So, MySQL has better optimize actions like retrieval, update and insert (talend, 2023).

### **2.3.8 Related Design Strategies**

Model-View-Controller (MVC) is a development pattern which makes independent model and view independent by connecting them together using controllers (SURABHI, 2022). CodeIgniter is a PHP framework based on this MVC architecture which will be used to create the system which helps to write clean and modular code.

In this model, all the data objects are in the models. When the user requests some service, it would be called by the controller. The controller transfers data from the model, process it and pass it to the View. This architecture can be integrated with the JavaScript Framework. The MVC design pattern is the best approach for developing web-based systems.

In this model, all the data objects are stored in the models. When the user requests some service, it is called by the controller. The controller transfers data from the model, process it and pass it to the View. This architecture can be integrated with the JavaScript Framework. The MVC design pattern is the best approach for developing web-based systems. CodeIgniter has been selected as the framework to develop this project since it is expertise by the author and it is good framework with the MVC Architecture. It has an active large community of developers who contribute to its growth and provide support to fellow developers. CodeIgniter is lightweight and fast, which makes it easy for developing high-performance web applications. When we consider about security aspect of CodeIgniter framework, it has in-built security features such as CSRF protection (VeraCode, 2018) SQL injection prevention and XSS filtering (Technologies, 2016). CodeIgniter works with almost all PHP versions and runs smoothly on various operating systems. Not only that, but also it has good documentation that helps its users to easily solve the problems when developing applications. By considering all these reasons, CodeIgniter framework has been selected for development to proceed further in this project.



## Chapter 3 – Design Architecture

### 3.1 Introduction

This chapter describes and provide details of design methods, detailed analysis of the technologies and the optimal way to develop user friendly and productive Network Firewall and Access Management System. This chapter provide the UML diagrams such as sequence diagrams, class diagrams and use case diagrams which illustrate the requirement analysis and the design of the final product.

### 3.2 System Architecture

System architecture refers to the way various components such as interfaces, middleware and databases organized and interact to achieve specific goal. In the context of a web application, system architecture outlines how the user interface, data processing, and server communication work together. As illustrated in Figure 3.1, system architecture defines how a web application's parts collaborate to deliver a seamless experience for users, ensuring everything runs efficiently, securely, and as intended. Application user will access the web application using given URL.

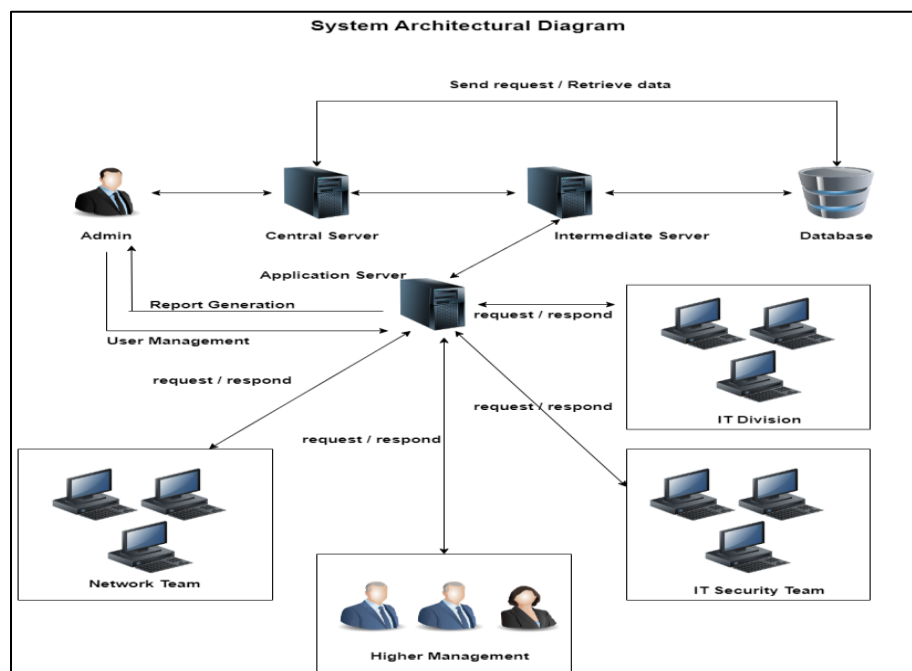
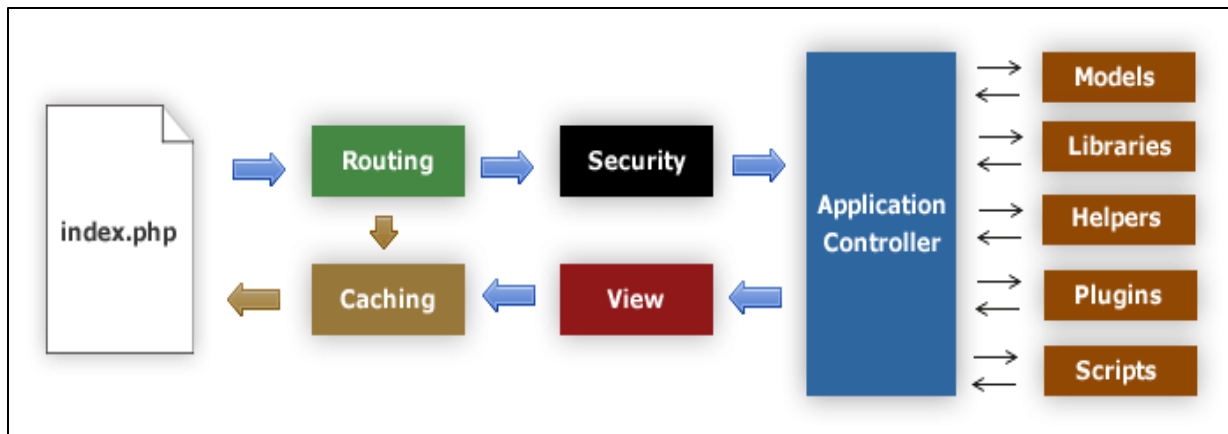


Figure 3.1: System Architecture Diagram

Basically, this web application contains two main components. The front-end and the back-end. System users directly interact with the front-end. The front-end is responsible for presenting information, responding to user actions, collect data from users, and creating an engaging user experience. Network Firewall and Access Management System front-end was written using the use HTML, CSS and JavaScript. Below are the request and response path process of how web application works on the client side.

- A user generates a request by typing in the web link (URL) in a browser's address bar.
- The browser sends request to the web server. This request contains various information, including the request method (e.g., GET, POST), the requested URL, headers, and sometimes data for POST requests.
- When the web server receive the request, server process the request. This involves locating the requested resource on the server's file system or generating dynamic content based on the request.
- After processing the request, the web server generates the response. Then web server sends the HTTP response back to the user's browser over the established TCP connection.
- The browser receives the Web server response and start processing it. If the response contains HTML, CSS, JavaScript, and other web assets, the browser renders the content accordingly. It lays out the page, applies styles, executes scripts, and displays any multimedia elements.

The backend of a web application is the part that operates behind the scenes and is responsible for handling data storage, business logic, and interactions with the database and external services. It handles the heavy lifting of data management, business logic, and interactions with databases and external services. It ensures that the frontend user interface functions properly by providing the necessary data and functionality.(Architecture, 2021)



*Figure 3.2: CodeIgniter Architecture*

- File **index.php** is the default file of CodeIgniter. It initializes the base resources.
- The **Router** decides what should be done with the information.
- If requested **cache** file exists, then the information is passed directly to the browser ignoring the further processes.
- Before loading Application Controller, the HTTP request and submitted data is passed under Security check.
- The Application Controller loads Models, Libraries, Helpers, Plugins and Scripts needed according to the request.
- The Application Controller loads Models, Libraries, Helpers, Plugins and Scripts needed according to the request.

### 3.3 UML Diagrams

#### 3.3.1 Use case Diagrams

Module wise use case diagrams for the five major modules in developed system.

- Use case diagram for administrative module

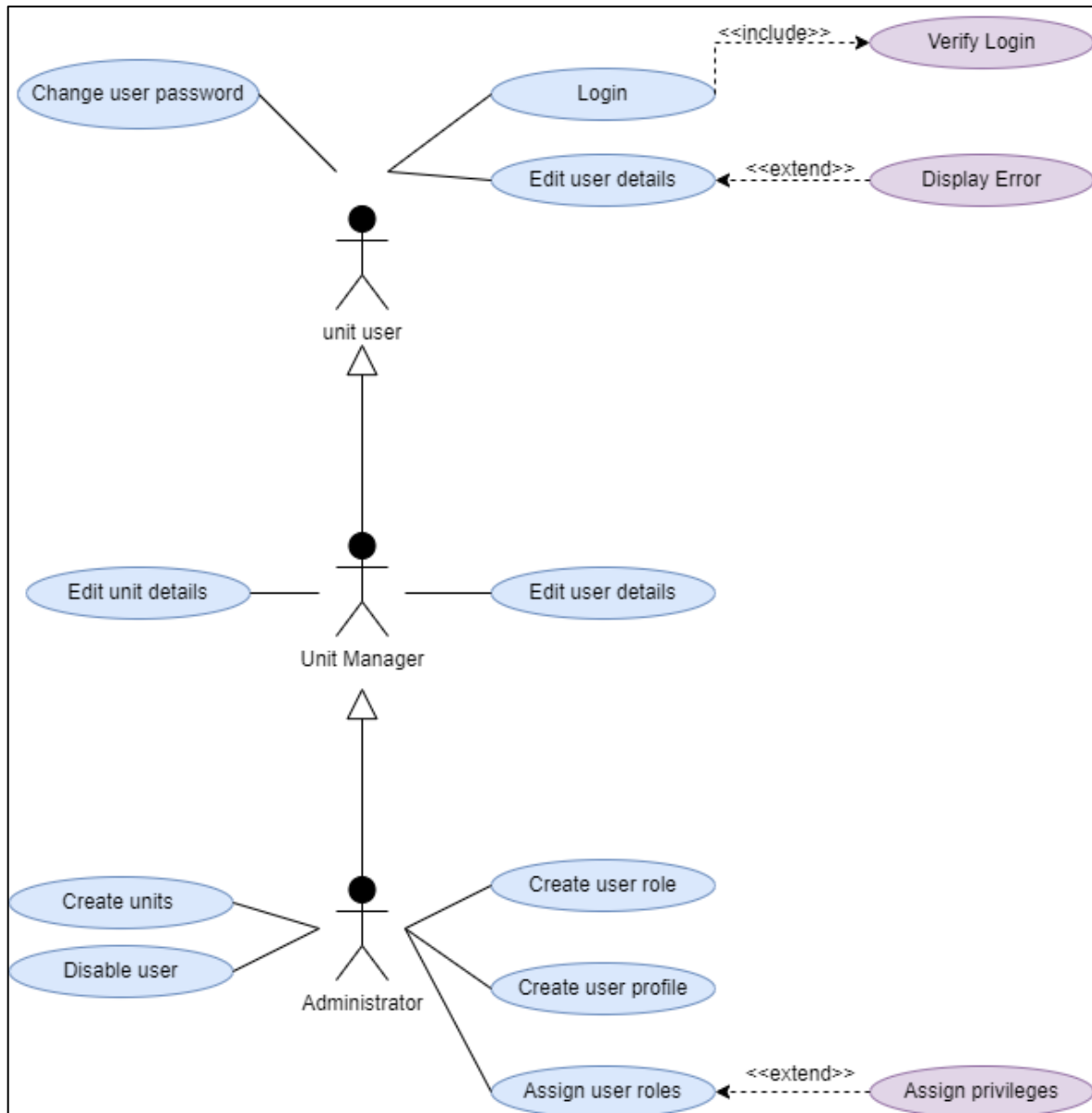


Figure 3.3: Use case diagram for administrative module

- Use case diagram for firewall port access module

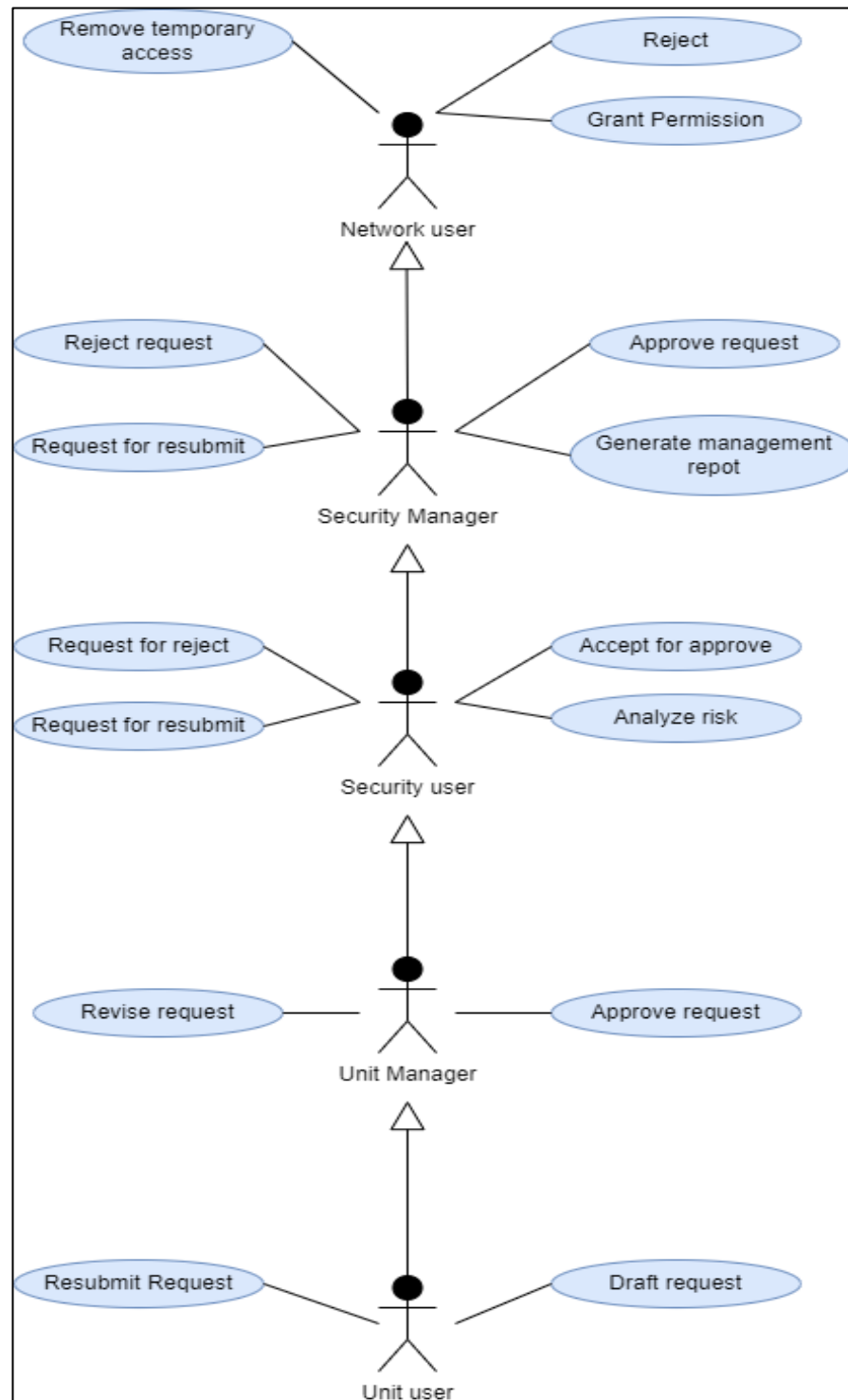


Figure 3.4: Use case diagram for firewall port access module

- Use case diagram for password reset module

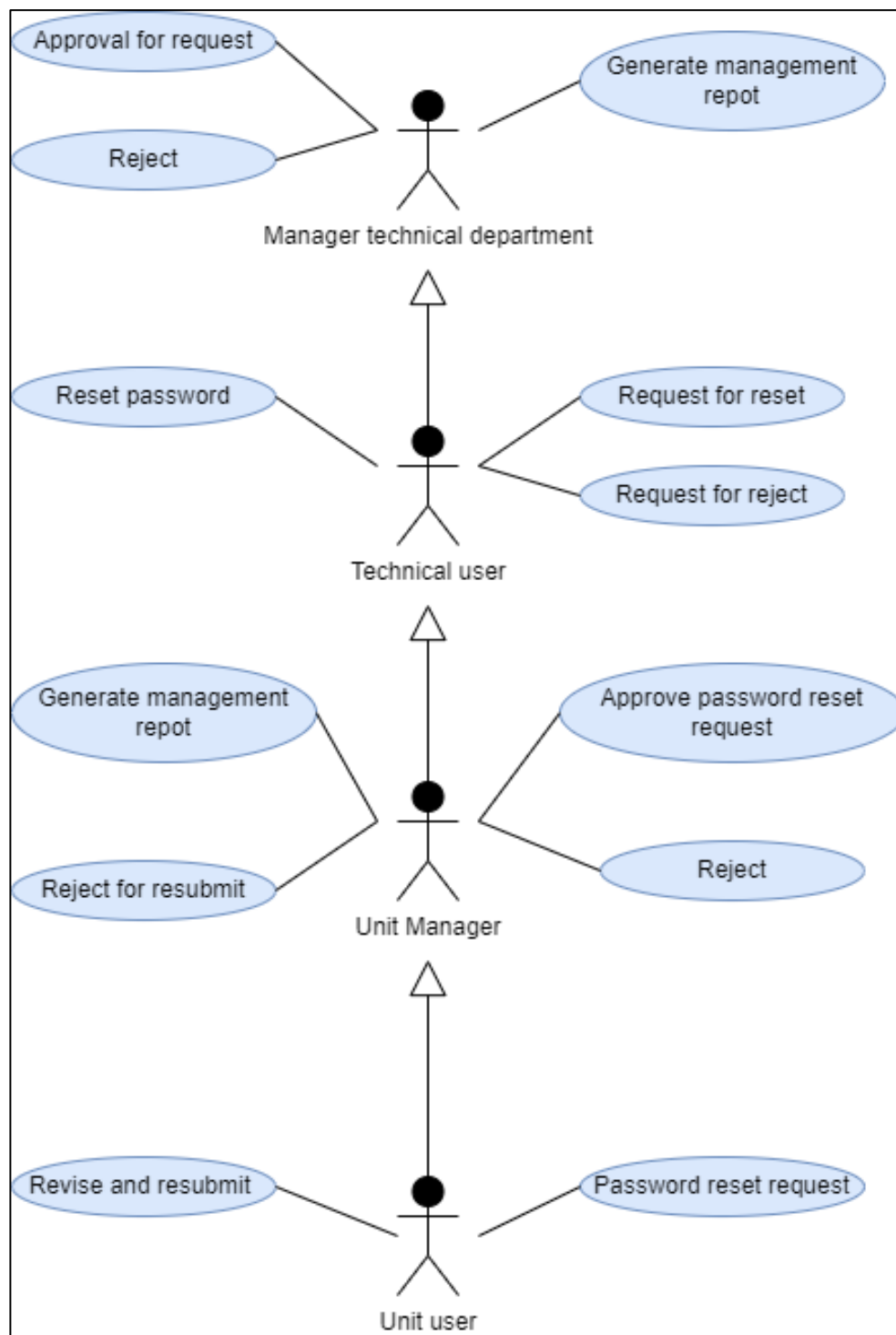


Figure 3.5: Use case diagram for password reset module

- Use case diagram for vulnerability management module

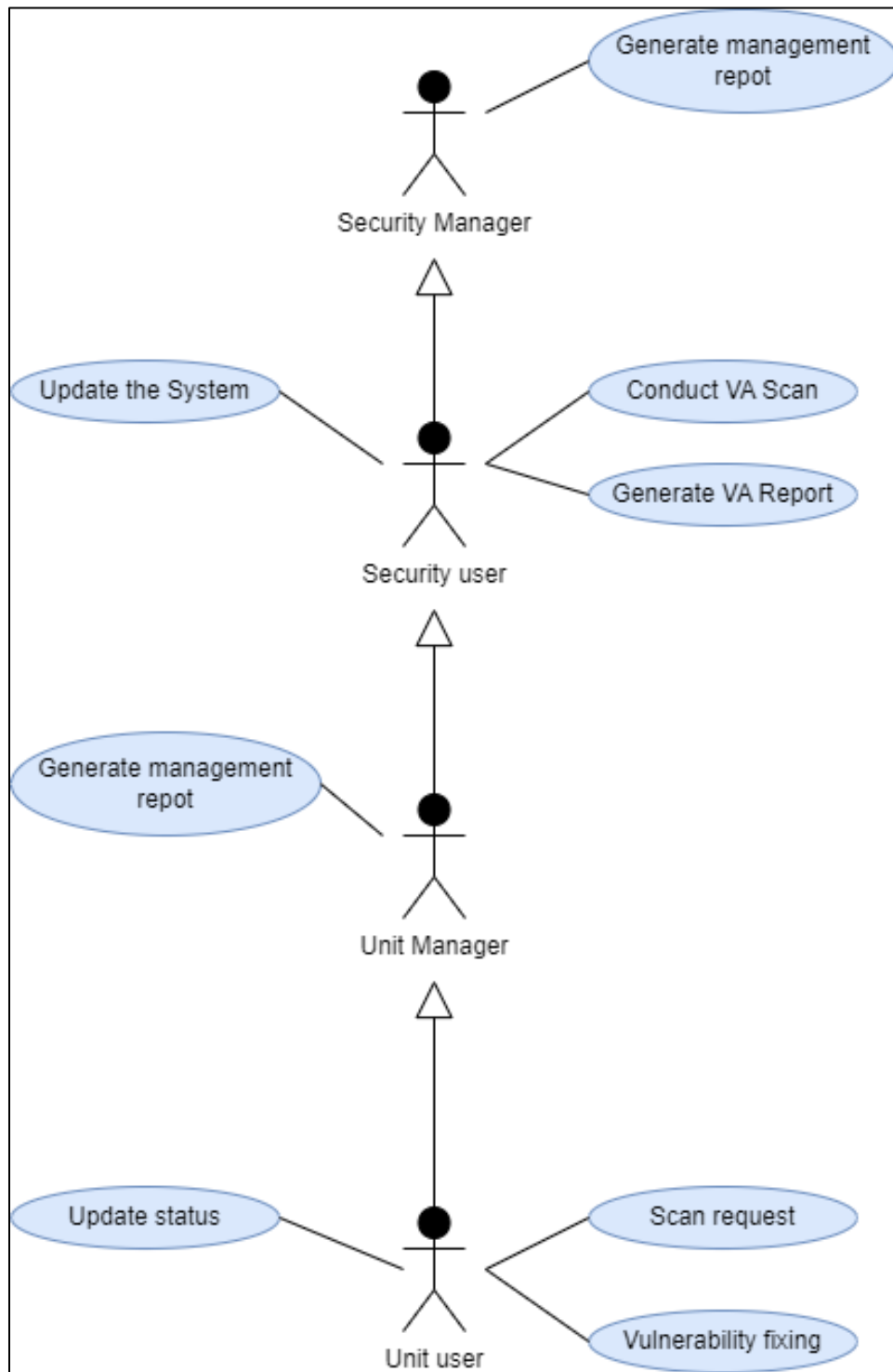


Figure 3.6: Use case diagram for vulnerability management module

- Use case diagram for reporting module



Figure 3.7: Use case diagram for reporting module



### 3.3.2 Use case narrations

Use case narrations for the main use cases in the above use case diagrams are shown below.

- Use case narration for login

Use case id	01	<u>Use case Type</u>  <b>Requirement:</b>  Prevent unauthorized access and authenticate user.
Use case name	Login	
Priority	High	
Source	Web Page – Login DB Table – User, Session	
Description	This use case allows user to login into the system to access the relevant functions according to the user’s role. The user roles are staff, system administrator, managers, security team, technical team, network team and the higher manager. Successful login the system will display the relevant user’s home page.	
Primary Actor	User	
Secondary Actor	None	
Other Interested Stakeholders		
Preconditions	User has to have a valid account	
Trigger	User send request to login by pressing the login button	
Typical course of events	1) User enter the username and password 2) Click on the Login button.	
Alternative course	Error message will be displayed for the invalid username or password entered by the user.	
Post conditions	Application will create a session and redirect the user to the relevant home page.	

Table 2: Use case narration for login

- Use case narration for create new user profile

Use case id	02	<b>Use case Type</b>  <b>Requirement:</b> Add new users to the system with relevant privileges.
Use case name	Create user profile	
Priority	High	
Source	Web Page – User Creation DB Table – User, ActionLog	
Description	Create user profile for the new users. After creating profiles user will able to login to the system. According to their user role features are available on the home page. Administrator will decide the user role for each user.	
Primary Actor	Administrator	
Secondary Actor	None	
Other Interested Stakeholders		
Preconditions	User has the administrative privileges to create new user profiles.	
Typical course of events	<div>1) User selects new user creation option available in the main menu.</div> <div>2) Enter the required details of the new user and assign the role group and department.</div> <div>3) Click on the save button.</div>	
Alternative course	<div>1) Application will display an error message if user have not entered any value for required field.</div> <div>2) Application will display an error message if the users provident fund number already exists in the application.</div> <div>3) Application will display a success message after creating the new user profile.</div>	
Post conditions	Default username will be user’s provident fund number and password will be the same which will be forced to change on the first login attempt.	

*Table 3: Use case narration for create new user profile*

- Use case narration for request new firewall request

Use case id	03	<u>Use case Type</u>  <b>Business Requirements:</b>  Draft new firewall request to IT security division
Use case name	Draft firewall request	
Priority	High	
Source	Web Page -Firewall request DB Table - Service_Request	
Description	Unit user submit a new Firewall request to the IT Security division through the Unit manager. Security team will analyze the risk and submit for approval to network team or reject the request, reject for resubmit.	
Primary Actor	Unit Manager, Security Team, Network Team	
Secondary Actor	Firewall Request	
Other Interested Stakeholders	Unit User, Developer	
Preconditions	Unit manager has the required manager privileges to submit a firewall request.	
Trigger	User selects “New firewall request” function from the menu items.	
Typical course of events	1) Enter the required details of the firewall request including correct IP Addresses, Date range and protocols.  2) User have to select the Unit Manager who will approve the firewall request before submitting to IT security division.	
Alternative course	1) Application will display an error message if user have not entered any value for required field.  2) Application will display a success message after submitting new DM request.	
Post conditions	Request will be displayed for the selected Unit Manager for their approval. Unit manager can reject the request or approve.	

Table 4: Use case narration for create new demand manager request

- Use case narration for password reset

Use case id	04	<u>Use case Type</u>  <b>Requirements:</b>  Reset password with log. Keep a track of status and approve or reject reset request by technical department.
Use case name	Password reset request	
Priority	High	
Source	Web Page – Password reset DB Table – Password_reset	
Description	After sending password reset request through the unit manager technical team attend on task. They check decide whether reset or reject the request.	
Primary Actor	Technical Department	
Secondary Actor	Unit Manager	
Other Interested Stakeholders	Higher Management	
Preconditions	Unit manager has the required manager privileges to request password reset from the technical team.	
Trigger	User select the password reset option from menu and provide necessary details. Assigned unit manager and press request button.	
Typical course of events	1) Select the reset request from the list. 2) View details and decide whether reset or not.	
Alternative course	System displays a success message after successfully password reset.	
Post conditions	Unit user can views the request status using system.	

*Table 5: Use case narration for password reset*

- Use case narration for Vulnerability Assessment request

Use case id	05	<u>Use case Type</u>  <b>Requirements:</b>  Unit user will request the VA assessment and they get the report with VA sttus.
Use case id	Request for vulnerability assessment	
Priority	High	
Source	Web Page – VA Request DB Table – VA_servicedata	
Description	Adding a Request for VA assessment, security team can view and attend the task. After Doing the VA scan security team will update the system.so requested user and management can view the VA status. Unit user will attend to fixing the vulnerability on servers.	
Primary Actor	Unit User	
Secondary Actor	Security Team, Unit manager	
Other Interested Stakeholders	Higher Management	
Preconditions	Unit manager has the required manager privileges to request VA assessment from the security team.	
Trigger	User selects the VA Request from menu and provide needed details submit after assign the unit manager.	
Typical course of events	1) Select the VA request from the list and conduct the VA scan  2) Update system with VA details and submit.	
Alternative course	If user provide incorrect details, Unit manager will reject the request.	
Post conditions	Once user post the message it will be displayed on the home screen of the knowledge management portal.	

*Table 6: Use case narration for Vulnerability Assessment request*

### 3.3.3 Sequence Diagrams

Sequence diagrams for the main use cases in the above use case diagrams are shown below.

- Sequence diagram for login

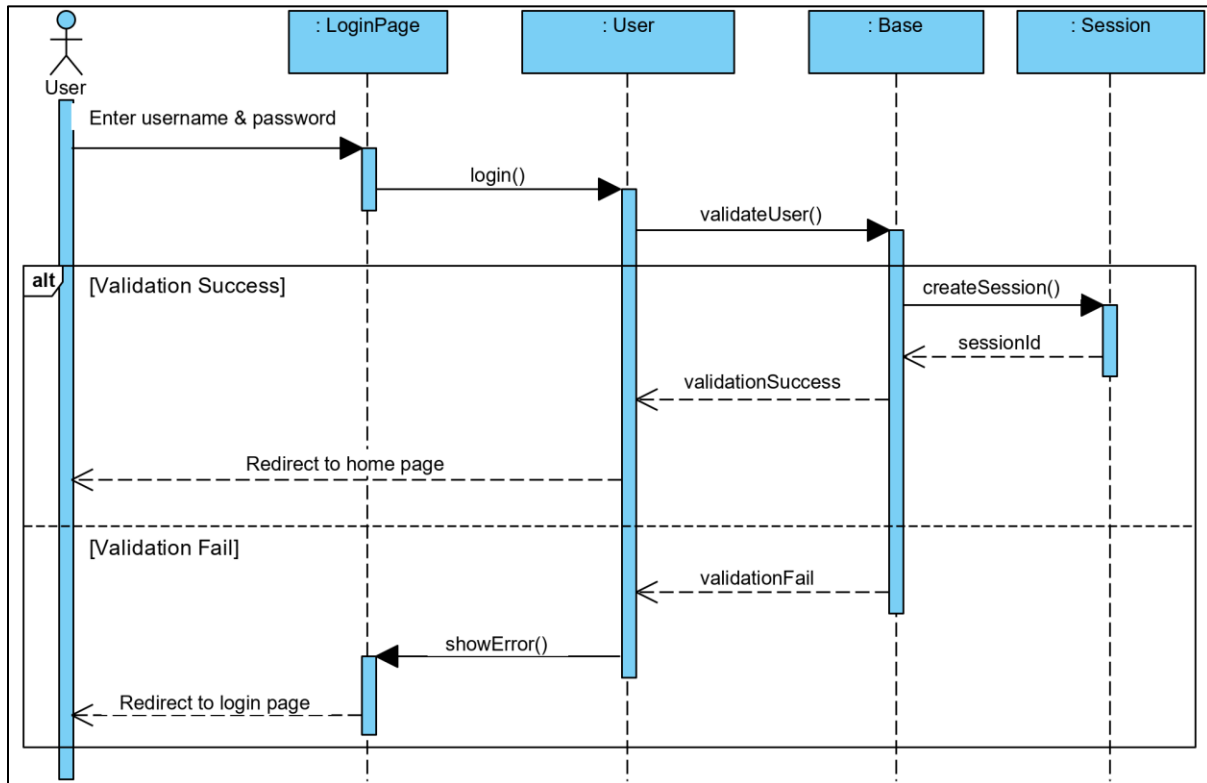


Figure 3.8: Sequence diagram for login

- Sequence diagram for create new user profile

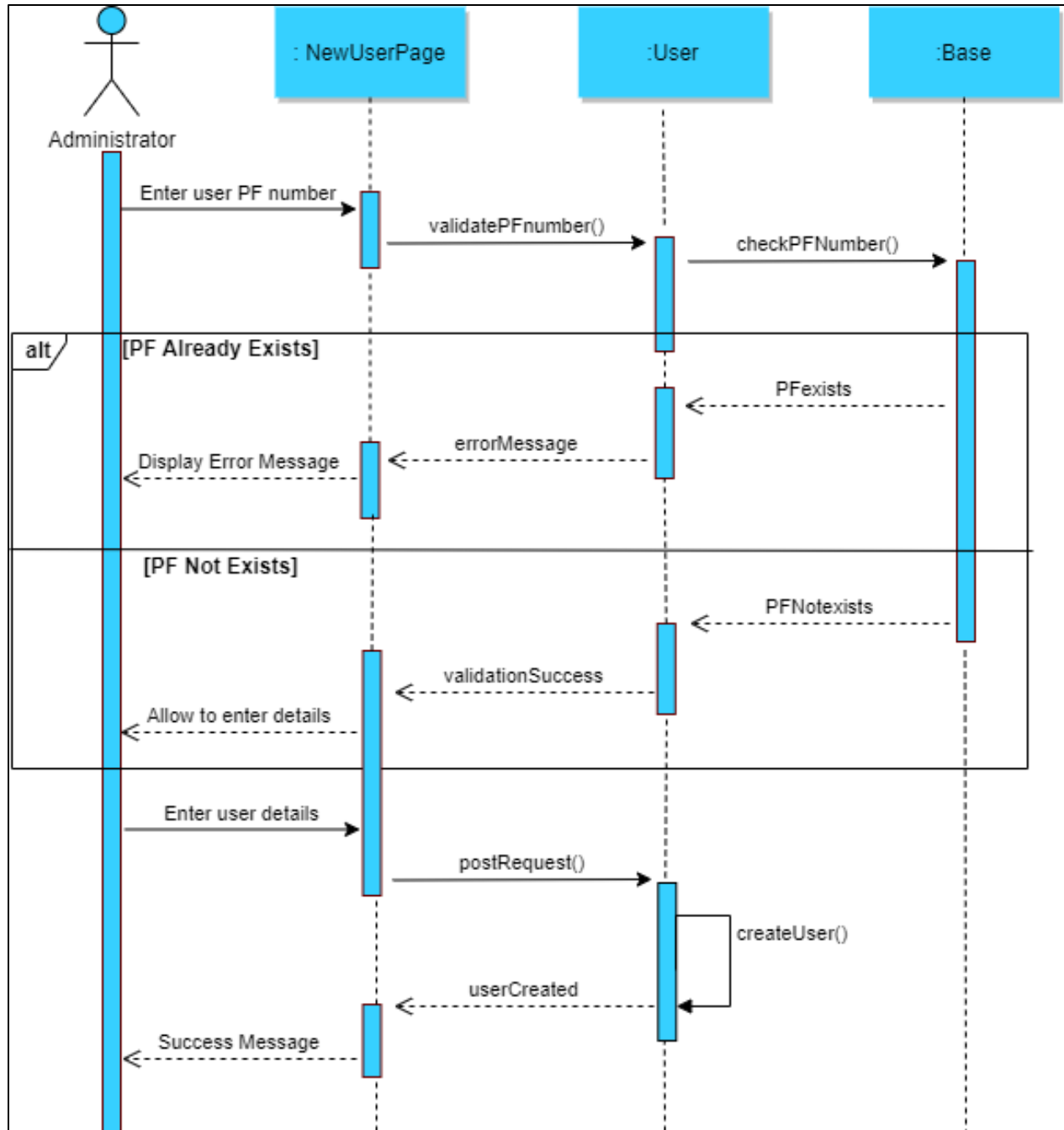


Figure 3.9: Sequence diagram for create new user profile

- Sequence diagram for create new firewall request

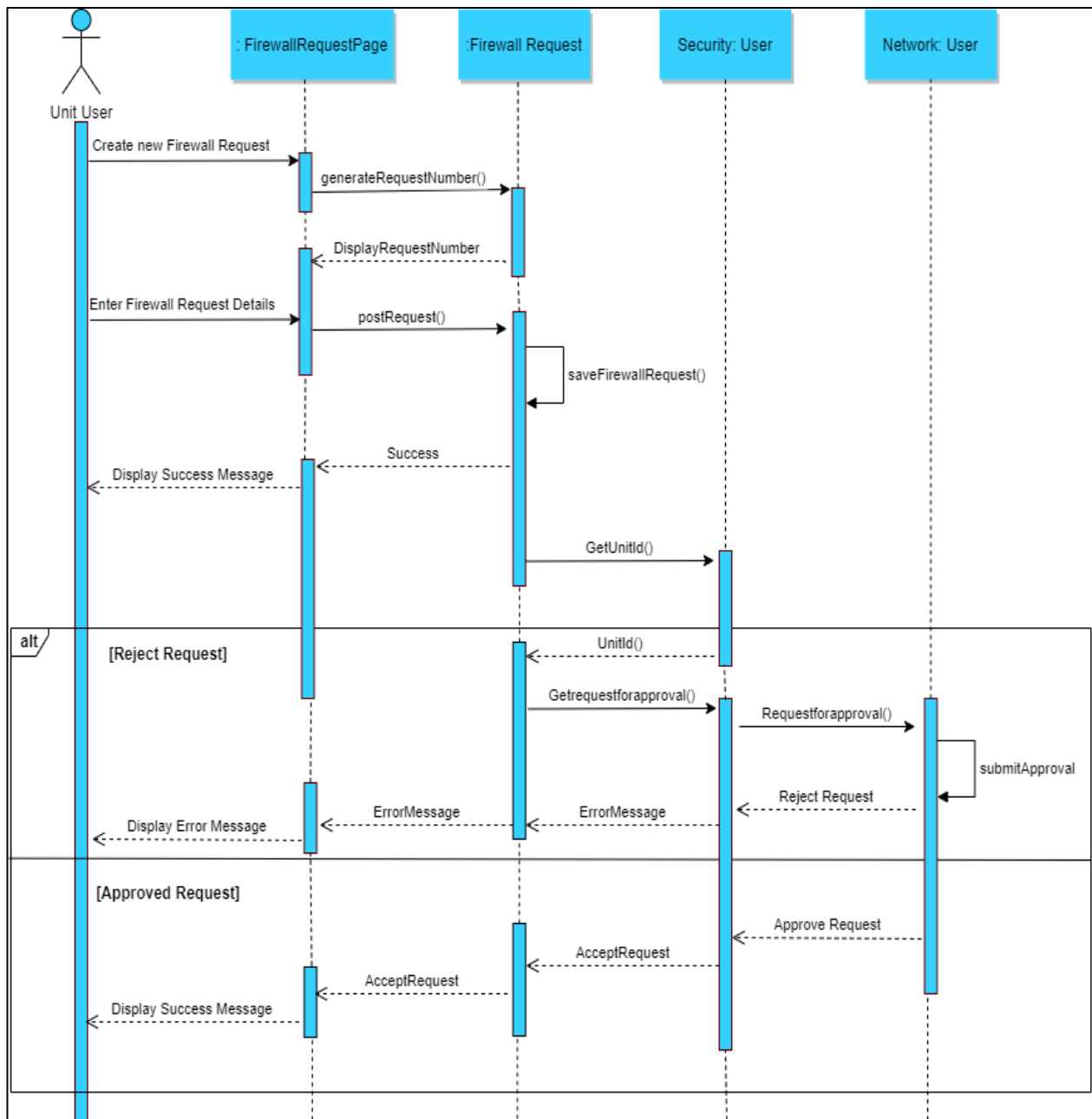


Figure 3.10: Sequence diagram for create new firewall request



### 3.3.4 Class Diagram

Class diagram for the developed Network and Firewall Management System.

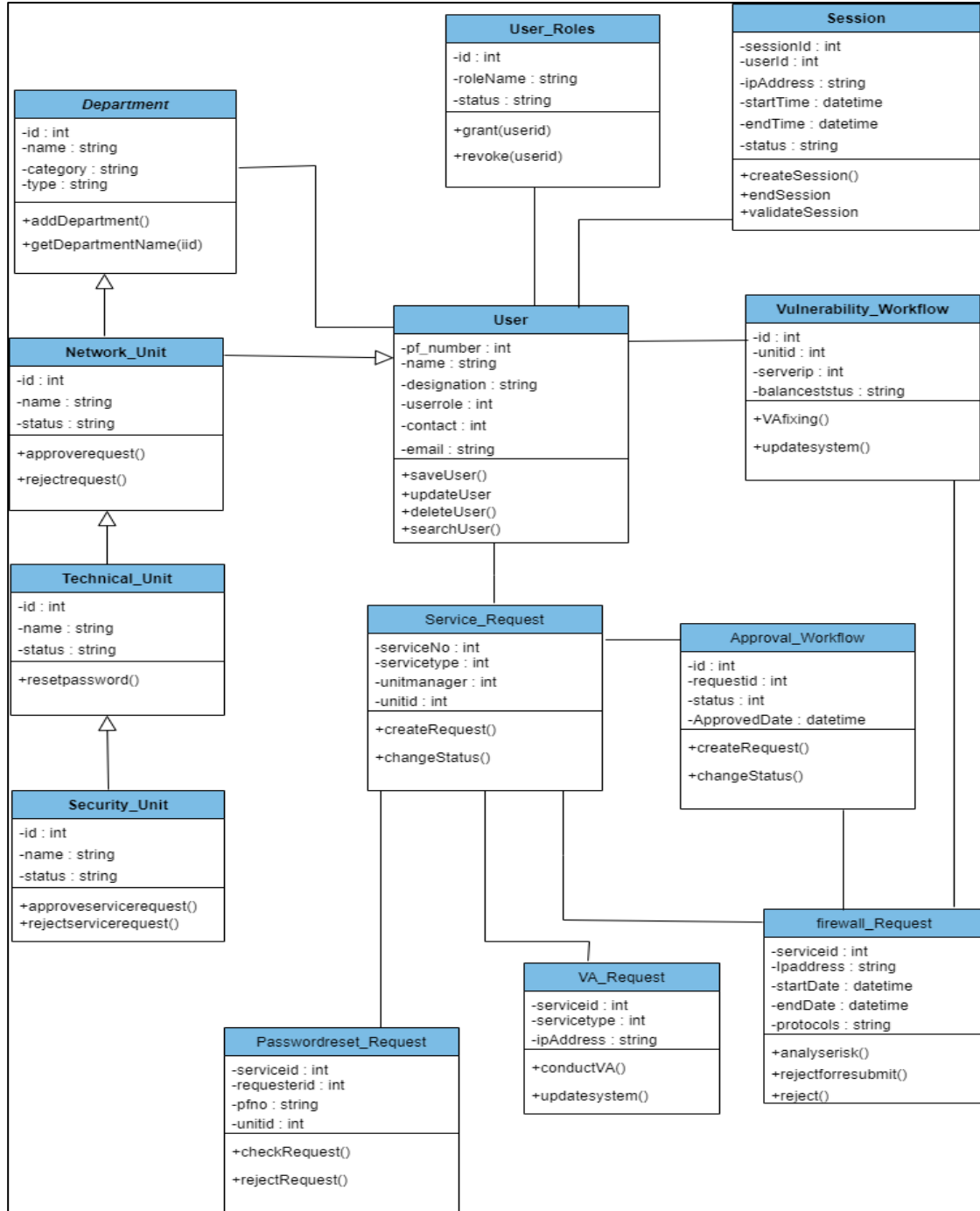


Figure 3.11: Class diagram of the web application

## Chapter 4 - Implementation

To develop the Web based system for Firewall and Access Management, different frameworks, technologies, and third-party components are used. So, it helps to develop user-friendly system. This section briefly explains the frameworks and technologies that are used to develop this solution.

For the development, Visual studio code has been used for coding PHP based web application. Design, Modification and maintenance of database were done by using the MySQL Workbench IDE. Those are the basic tools that were used in the development phase.

### 4.1 Architecture of Implementation

MVC (Model-View-Controller) architecture is the architecture that was used to develop this solution. (Hernandez, 2021)MVC separates the application into three main logical components Model, View and the Controller. As discussed in the earlier chapter, Model contains the data logic, View contains the GUI (Graphical user Interface) and controller acts as the brain of the application. The graphical view of the folder structure is shown in Figure 4.1 below.

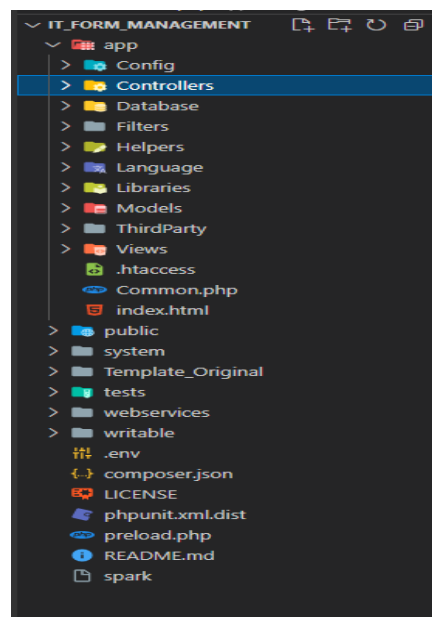


Figure 4.1: Folder Structure

Mainly fresh CodeIgniter projects have five directories app, public, writable, tests and vendor or system. Each of these have unique role to play. (CodeIgniter Foundation, 2019)

- App – this is the heart of the application. Because that is the directory that live all of application code. This directory again contains some of sub directories.
- Config - It contains application configurations. It includes all the important configuration files like Routes, Database etc. Routes.php includes the directions for interfaces. Sample of routing syntax that use in the application are shown in Figure 4.2.

```
$routes->get('/', 'Login::index');
$routes->post('/login', 'Login::login');
$routes->get('/logout', 'Login::logout');

$routes->get('/dashboard', 'Home::home');
$routes->get('/requests/new', 'Firewallrequest::addnew');
$routes->post('/requests/save', 'Firewallrequest::save');
$routes->get('/requests/pendingrequest', 'Firewallrequest::pendingrequestlist');
$routes->get('/requests/approve', 'Firewallrequest::approval');
$routes->get('/authentication/authorise', 'Firewallauthentication::authenticationpanel');
$routes->get('/authentication/approve', 'Firewallauthentication::authentication');
$routes->get('/requests/getpendingitem/(:any)', 'Firewallrequest::getselectedreq/$1');
$routes->post('/requests/approval/(:num)', 'Firewallrequest::approvebyman/$1');
$routes->get('/requests/getauthitem/(:any)', 'Firewallauthentication::getselectedauthreq/$1');
$routes->post('/authrequests/approval/(:num)', 'Firewallrequest::approvebyitsec/$1');
// $routes->get('/authentication/authorise', 'Firewallrequest::pendingrequestlist');

$routes->setAutoRoute(true);
```

Figure 4.2: Routing syntax

- Application use the Database.php file to connect with the database. The Content of the Database.php file are shown in Figure 4.3 below.

```

/**
 * The default database connection.
 *
 * @var array
 */
public $default = [
    'DSN' => '',
    'hostname' => 'localhost',
    'username' => 'root',
    'password' => 'P@ss6ook@admin',
    'database' => 'itformmanagement',
    'DBDriver' => 'MySQLi',
    'DBPrefix' => '',
    'pConnect' => false,
    'DBDebug' => (ENVIRONMENT !== 'production'),
    'charset' => 'utf8',
    'DBCollat' => 'utf8_general_ci',
    'swapPre' => '',
    'encrypt' => false,
    'compress' => false,
    'strictOn' => false,
    'failover' => [],
    'port' => 3306,
];

```

Figure 4.3: Content of database.php

- Controllers – It determines the program flow. It acts as the brain to process models and display the views making an application working flow.
- Database - Stores the database migrations and seeds files.
- Filters - Stores filter classes that run before and after controllers
- Helpers - This folder includes all the helper classes of the application.
- Language - Multiple language support reads the language strings from here.
- Libraries - Useful classes that don't fit in another category.
- Models - Models work with the database to represent the business entities.
- ThirdParty – Third party libraries that can be used in application.
- Views - Views make up the HTML that is displayed to the client.
- Public – This folder is introduced in CodeIgniter 4 Version. It contains index.php, .htaccess, publicly accessible folders and/or files. At initial stage, application runs from this folder. In the application development, it is needed to keep assets like CSS, JS, and Images etc. in the public folder. Its name means publicly accessible folder.

- **System** - This directory stores the files that make up the framework, itself. The files in the system directory should never be modified. Instead, extended classes, or creating new classes, to provide the desired functionality could be done.
- **Tests** – This directory holds the test files. The support directory holds various mock classes and other utilities that are used for writing tests. This directory does not need to be transferred to production servers.

## **4.2 Query Builder Class**

CodeIgniter 4 framework provide the inbuilt Query build class. Using this inbuilt class data can be inserted, retrieved, and updated to the database with minimal scripting. Rather than few lines of query, the same result can be obtained by using one or two lines. In CodeIgniter, there's no necessity for individual class files dedicated to each database table; instead, it offers a more streamlined and straightforward approach. This Query Builder Class provides a safe and flexible way to work with databases in PHP applications. In this method we call the database class by query builder class via the controller class. The sample of Query executer for insert operation using the query builder class are shown in Figure 4.4.

```

public function save()
{
    // $data = trim($this->request->getVar('changetype'));
    // var_dump($data);die;
    $requestdata = [
        "staffmember" => trim($this->request->getVar('name')),
        "pfno" => trim($this->request->getVar('pfno')),
        "email" => trim($this->request->getVar('email')),
        "mobile" => trim($this->request->getVar('mobile')),
        "extention" => trim($this->request->getVar('exten')),
        "date" => trim($this->request->getVar('request_date')),
        "department" => "IT",
        "position" => 1,
        "approvedby"=>"IT",
        "typeofchange" => trim($this->request->getVar('changetype')),
        "category" => trim($this->request->getVar('category')),
        "effectdate" => trim($this->request->getVar('effec_date')),
        "expiredate" => trim($this->request->getVar('expire_date')),
        "explanation" => trim($this->request->getVar('explanation')),
        "source" => trim($this->request->getVar('source')),
        "destination" => trim($this->request->getVar('destination')),
        "protocol" => trim($this->request->getVar('protocol')),
        "ports" => trim($this->request->getVar('ports')),
        "direction"=> trim($this->request->getVar('direction')),
        "action" => trim($this->request->getVar('action')),
    ];

    $result = $this->firewallrequest->saveRequest($requestdata);

    if ( $result > 0 ) {
        var_dump("saved successfully");
    } else {
        var_dump("save error!");
    }
}

```

Figure 4.4: Insert Query in Query Builder

### 4.3 Look and Feel of the web application

To maintain Attractive and user-friendly interface the custom build template has been used. Because look and feel of a web application are critical factors that influence user engagement and satisfaction. In this web application open-source template has been used. Customized sample of web page is shown below.

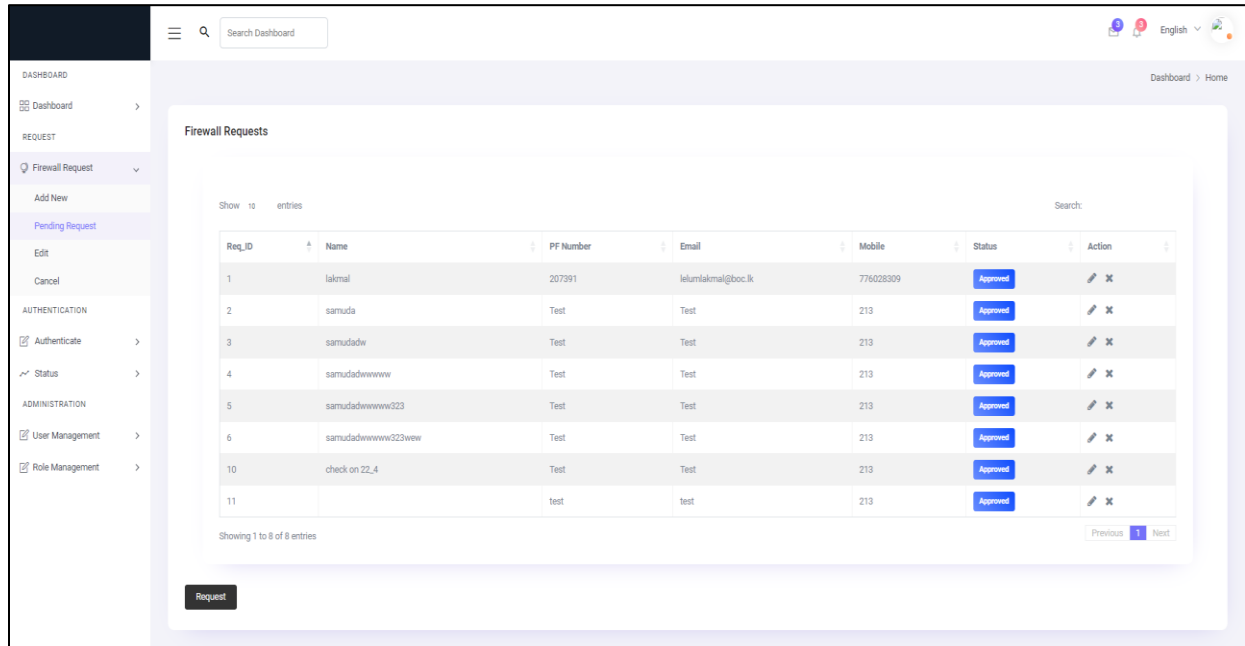


Figure 4.5: Sample web page

In this design, the web page is divided to three main sections. Main menu, header, and content section. The header, footer and main menu are common for the each and every page in the application it was created as four separate PHP files as baselayout.php, sidemenu.php, and content.php.

# **Chapter 5 – Testing and Evaluation**

## **5.1 Introduction**

Testing is a systematic process to guaranteeing that the developed application adheres to quality standards and aligns with customer requirements. It will be used to validate the system which problems that could affect. This includes looking for things that might make the application slow or cause it to not work correctly. This chapter outlines the comprehensive testing plan for the web application that has been developed. End of this process it evaluates whether the project objectives have been met through the development process.

## **5.2 System Testing**

To deliver quality product, a strong testing plan is crucial for detecting and resolving issues before the application is deployed for use. Throughout the system testing process, communication and collaboration between testers, developers, and stakeholders are crucial. It works properly, delivers on its promises, and fulfils the customer requirements. Software Quality Assurance is a set of activities that verifies a system to identify whether the system meets its user requirements. In this scenario decide to conduct unit resting during the development by separating major function from other component to testing individually for inputs and outputs.

In the waterfall model, Integration Testing is a critical phase where individual components of an application are combined and tested together as a group. The integration testing is to verify that the interactions between these units or components work as expected when integrated. In this phase mainly target to test the data flow through the integrated system and ensure that interfaces between units and modules work as intended.



Unit testing is used in the first phase to test each individual module and component separately, as specified in the test plan. Unit testing is finished before integration testing starts. Integration testing involves methodically integrating each component one at a time until every module is integrated and tested as a whole.



### 5.2.1 Test Cases

The following list contains the test cases that were used to evaluate the created Network Firewall and Access Management System, as shown in Table 7.

- Test Cases for Login

ID	Activity	Steps in a Test Case	Expected Result	
1.1	Use a legitimate user account to log in.	Visit <a href="http://localhost/IT_form_management/public/">http://localhost/IT_form_management/public/</a>	User able to access the login page	
		Input valid username and password	Both fields should be accessible to the user.	
		Click on Login	Successful login	
1.2	Leave the password field empty with legitimate username to log in.	Visit <a href="http://localhost/IT_form_management/public/">http://localhost/IT_form_management/public/</a>	User able to access the login page	
		Input user name only and keep password empty	Both fields should be accessible to the user.	
		Click on Login	Error message indicating that "Enter Both Field"	
1.3	Leave the username field empty with correct password to log in.	Visit <a href="http://localhost/IT_form_management/public/">http://localhost/IT_form_management/public/</a>	User able to access the login page	
		Input password only and keep username empty	Both fields should be accessible to the user.	
		Click on Login	Error message indicating that "Enter Both Field"	

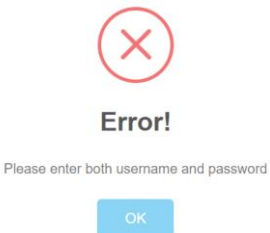
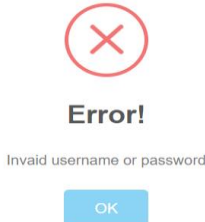
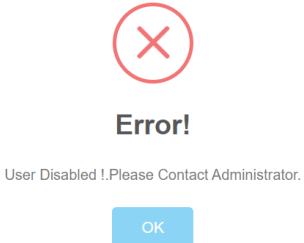
1.4	Login with both empty username and password	Visit <a href="http://localhost/IT_form_management/public/">http://localhost/IT_form_management/public/</a>	User able to access the login page	
		Leave both username and password empty	Both fields should be accessible to the user.	
		Click on Login button	Error message indicating that “Enter Both Field”	
1.5	Use an invalid credentials to log in.	Visit <a href="http://localhost/IT_form_management/public/">http://localhost/IT_form_management/public/</a>	User able to access the login page	
		Use invalid credentials for login	User able to access the login page	
		Click on Login button	Error message indicating that “Invalid Credentials”	
1.6	Use a legitimate password and username with “Disabled” status to login	Visit <a href="http://localhost/IT_form_management/public/">http://localhost/IT_form_management/public/</a>	User able to access the login page	
		Use valid credentials for login	Both fields should be accessible to the user.	
		Click on Login button	Error message indicating that “User deactivated”	

Table 7: Test cases for login

- Test Cases for User Registration

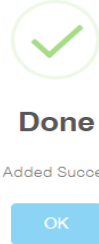
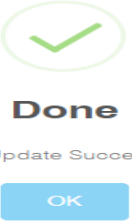
ID	Activity	Test Case Steps	Expected Result
2.1	Fill all needed field and add New User	Go to the User Management and select on Add, then add the details and submit	<p>User has been created successfully.</p> 
2.2	Fields Validations	PF Number Can't be empty	<p>Relevant Error message will display</p> <p>PF No</p> <input type="text"/> <p>The PF No field is required.</p> <p>Email</p> <input type="text" value="ssss334"/> <p>The Email field must contain a valid email address.</p>
		Check for already registered PF No	
		Mobile Number Field Can't be empty.	
		Email Address Should be valid email format and can't be null	
2.3	Update User	<p>PF No Cannot be updated.</p> <p>Enabled field should validate</p>	<p>Request should be successfully submitted.</p>
		Enter all relevant field accurately	<p>Should display a success message</p> 

Table 8: Test cases for user registration

### 5.2.2 Testing Status

Test ID	Description	Pass / Fail
1.1	Use a legitimate user account to log in	Pass
1.2	Leave the password field empty with legitimate username to log in.	Pass
1.3	Leave the username field empty with correct password to log in.	Pass
1.4	Login with both empty username and password	Pass
1.5	Use an invalid credentials to log in.	Pass
1.6	Use a legitimate password and username with “Disabled” status to login	Pass
2.1	Create new user screen	Pass
2.2	Check Validations	Pass
2.3	Update User	Pass

Table 9: Status of test cases

Detail test plan is mentioned in the Appendix D with all the other test cases and test results.

## 5.3 System Evaluation

Once the new system has been implemented, it should be evaluated. There is number of techniques available to evaluate the system. In evaluation process it considers the effectiveness, efficiency, performance, and the overall functionality of the developed system. For the evaluation of the developed Network Firewall and Access Management System. For newly developed Network Firewall and Access Management System, chose the criteria-based assessment which is quantitative assessment of the software in terms of maintainability, usability, and sustainability. Users who took part in the testing phase were given a questionnaire to complete to collect quantitative input on the software system's operation and appearance. The purpose of the questionnaire was to get structured answers.

Using virtual server machine UAT environment setup and the URL is shared among the selected unit of IT department. It is about 50 people selected from IT department. 5 persons from higher management and 45 persons from selected different units. After allowing selected users asked to use the system for time of one week to become familiar with the system. During this period prepare questionnaire by mainly focus on two aspects. In Questionnaire mainly focus on functionality and user experience of its visual design of developed system created using google forms. Excluding higher management every user asked to fill questionnaire on end of the one-week time.

Multiple questions about the produced web application were included in Questioner's design, and users can rate each inquiry. It will be simple to analyze data and assess user rating because each question has a number rating. There are five levels on the scale for questions, ranging from Strongly Disagree to Strongly Agree (1 to 5).

<h2 style="margin: 0;">Network Firewall and Access Management System</h2> <div style="display: flex; align-items: center; justify-content: center; margin-top: 10px;"> <div> <h1 style="margin: 0;">FIRENET360</h1> <p style="font-size: 0.8em; margin: 0;">NETWORK FIREWALL &amp; ACCESS MANAGEMENT SYSTEM</p> </div> </div>					
<p>We value your feedback to help us improve our Network Firewall &amp; Access Management System. Please take a few moments to share your thoughts with us</p>					
Name :	<input style="width: 90%;" type="text" value="Your answer"/>	Unit :	<input style="width: 90%;" type="text" value="Select your unit *"/>		
			Very Poor	Poor	Neutral
			Good	Excellent	
			1	2	3
			4	5	
Q3	How satisfied are you with the user interface and overall design of the Network Firewall & Access Management System *				
Q4	How easy it for you to add security/network request and follow them ? *				
Q5	Rate the performance and responsiveness of the overall the system in loading dashboards and reports *				
Q6	Rate the effectiveness of Network Firewall & Access Management System in helping you to identify the pending and completed request *				
Q7	How satisfied are you with the accuracy and reliability of the information display in the Network Firewall & Access Management System *				
Q8	The system is more efficient than the manual processHow satisfied are you with the level of integration and compatibility of the system with different browsers?(Microsoft Edge, Chrome and Firefox) ? *				
Q9	Rate the support and guidance provided by the system when filling a IT security and network request *				
Q10	How well do the validation checks and error fonts prompts display to the user *				
Q11	Rate the level of user role management and access controls implemented in the system to prevent unauthorised actions and data tampering *				
Q12	How would you rate the reliability and uptime of the network and security systems ? *				
Q13	How satisfied are you with the performance of the Network Firewall & Access Management System *				
<p>Do you have any other comments regarding the IT Form Management system?</p> <div style="border: 1px solid black; height: 30px; width: 100%; margin-top: 5px;"></div>					

*Figure 5.1: Evaluation Form*

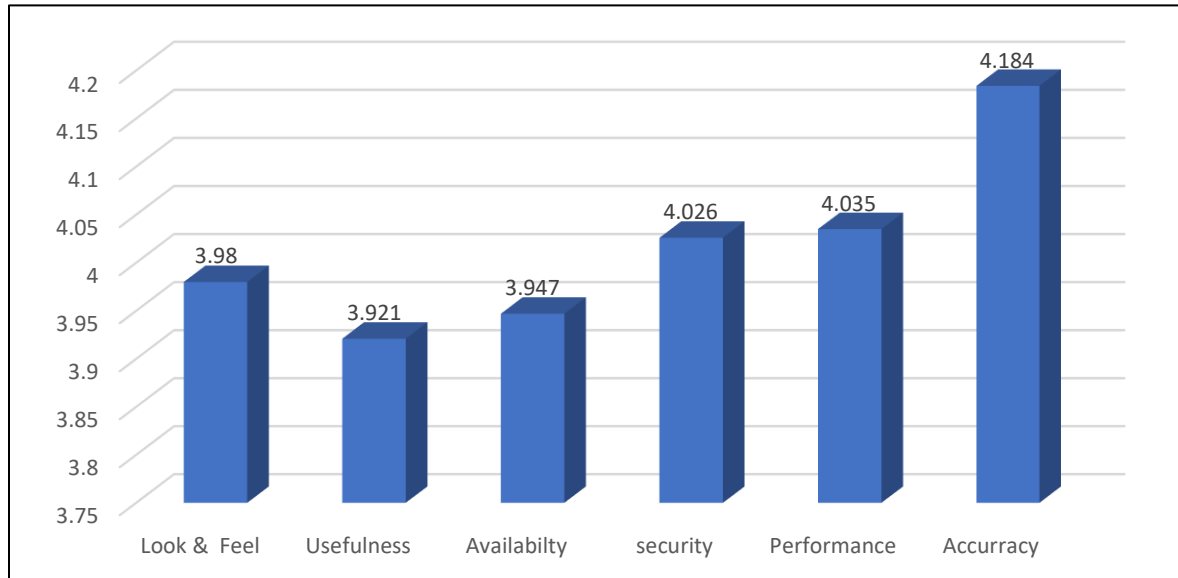
Sample google evaluation form which was given to the system users are shown in the figure 5.1. Share the google form within the selected users to fill end of the given time.

## 5.4 Analysis of the Results

Timestamp	1. Name	2. Unit	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13
2/26/2024 16:01:41	Madushi Seneviratne	General Application	4	4	4	4	4	4	4	4	4	4	4
2/26/2024 16:03:05	Diwanika	General Application	5	5	5	5	5	5	5	5	5	5	5
2/26/2024 16:04:13	Mithika	Internet Banking	5	5	5	5	4	4	5	5	5	4	5
2/26/2024 16:06:58	Ranga Perera	Core Development	3	2	3	3	4	2	3	3	4	4	3
2/26/2024 16:07:52	Saminda jayakody	Internet Banking	5	5	5	4	4	5	4	5	5	5	4
2/26/2024 16:13:28	Jananie Perera	Core Maintenance	3	3	2	3	3	3	3	3	3	4	3
2/26/2024 16:13:33	Kushan Jayasuriya	Internet Banking	3	2	3	3	3	3	3	3	3	2	2
2/26/2024 16:14:37	Chinthaka	ATM	4	4	4	5	4	5	5	4	5	4	4
2/26/2024 16:18:40	R.M.L.D. Rathnayake	Core Development	5	4	4	5	5	5	5	4	5	5	5
2/26/2024 16:22:58	Thilini Anoratna	Card Center	4	4	3	4	5	4	5	3	4	4	5
2/26/2024 16:24:22	Ishara Dilrukshi	Internet Banking	3	4	4	3	4	4	3	3	3	3	3
2/26/2024 16:33:10	Ielum	General Application	5	5	5	5	5	2	2	2	1	1	2
2/26/2024 16:34:13	Iresha Hearth	Internet Banking	3	3	3	3	3	4	3	3	3	3	3
2/26/2024 16:42:05	W. S. N. Perera	ATM	5	4	5	3	5	5	4	5	4	5	4
2/26/2024 16:52:52	Dilki Ishara	Internet Banking	4	3	4	4	4	4	4	3	3	4	3
2/26/2024 16:59:25	Dasun Tharuka	General Application	5	4	5	4	4	5	4	4	4	5	5
2/26/2024 16:59:51	Samuda Abeynayake	Core Development	5	5	5	5	4	4	4	5	5	5	4
2/26/2024 18:07:12	Pumima Deshani	Technical Support	3	3	3	2	4	4	4	3	5	4	4
2/26/2024 19:10:39	T. Y Diyawadanage	IT Security	5	5	5	5	5	4	5	4	5	5	5
2/26/2024 19:50:32	Thanuri Perera	Card Center	4	2	4	2	2	2	2	4	4	4	2
2/26/2024 20:30:13	Charitha	Technical Support	2	3	3	3	4	3	3	3	3	3	4
2/26/2024 20:37:58	Anjalie	Core Maintenance	5	4	4	3	4	4	4	3	4	3	4
2/26/2024 20:55:12	NPP Ranasinghe	Product And Services	3	4	4	3	4	5	3	4	4	3	4
2/26/2024 20:59:24	Hansi Piyumali	General Application	3	4	3	3	4	3	3	3	3	4	4
2/27/2024 0:01:54	Madumi	Card Center	5	5	4	4	5	5	5	5	4	4	5
2/27/2024 7:33:57	B.M.H.Shyamali	Internet Banking	5	5	4	5	4	4	4	4	4	4	5
2/27/2024 8:00:30	Supun Illangakoon	Internet Banking	4	3	3	3	4	4	4	3	4	4	4
2/27/2024 8:01:09	Maljinee Dayananda	Core Maintenance	3	1	3	1	2	3	1	2	3	2	3
2/27/2024 8:48:17	Janani	General Application	4	4	5	5	5	5	5	5	5	5	5
2/27/2024 9:16:06	Ayesh Ruwantha	ATM	4	4	4	4	4	4	4	3	4	4	3
2/27/2024 11:11:22	Piyumi	Technical Support	5	4	4	5	5	5	5	5	4	4	5
2/27/2024 12:58:26	Sachin Perera	IT Security	5	5	4	4	5	4	4	4	4	4	4
2/27/2024 13:04:40	M. M. V. Senanayake	General Application	4	4	4	4	4	4	4	4	4	4	4
2/27/2024 16:13:06	R M Buddhakorala	Internet Banking	5	5	4	5	5	5	4	5	4	5	4
2/28/2024 6:25:04	Chathura Dulanga	Technical Support	4	5	4	5	5	5	5	4	4	5	5
2/28/2024 6:52:26	Achini Perera	Internet Banking	5	5	5	5	5	5	5	5	5	3	5
2/29/2024 0:23:55	Dinesh	Technical Support	5	4	4	5	4	4	5	4	5	4	5
3/1/2024 21:02:43		Core Development	5	5	5	5	5	5	5	5	5	5	5

Table 10: Evaluation Results

Here is the result of the user responses for the given google form regarding the developed Network Firewall and Access Management System. After the user submission, the responses were collected to analyze the data. Using this collected data mean value for each question was calculated.



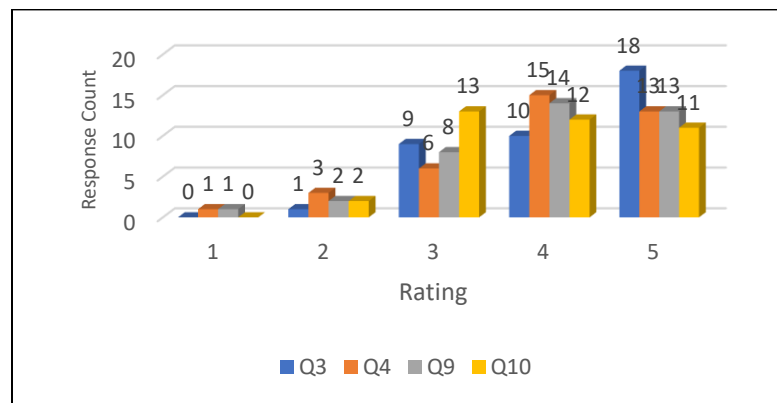
*Figure 5.2: Graph for category wise rating*

This figure 5.2 displays a graphic representation of the category-wise mean value that was determined using the user's evaluation. The following is a description of the major points that were found after examining the evaluation results.



- Look and feel

Question no 3<sup>rd</sup>, 4<sup>th</sup>, 9<sup>th</sup>, and 10<sup>th</sup> represent data on look and feel category. It collects data, user experience on interfaces, User-friendliness of interface and support guidance with validation on feeding data. It has received a rating of 3.98 as the mean of overall feedback for look and feel category. Below is the feedback chart for look and feel category. Over the 4 Question it gets 3.98 rating mean users are happy with the design.



*Figure 5.3: Rating on Look & Feel of the website*

- Performance

Question no 5, 8 and 13 collect the user feedback against the performance category. For the Performance category it has received a rating of 4.035, as illustrated in Figure 5.4. In this category user able to share their experience on Compatibility of the system with different browsers and overall satisfaction of the developed system. Therefore, it can be concluded that system performance meets the user expectation.

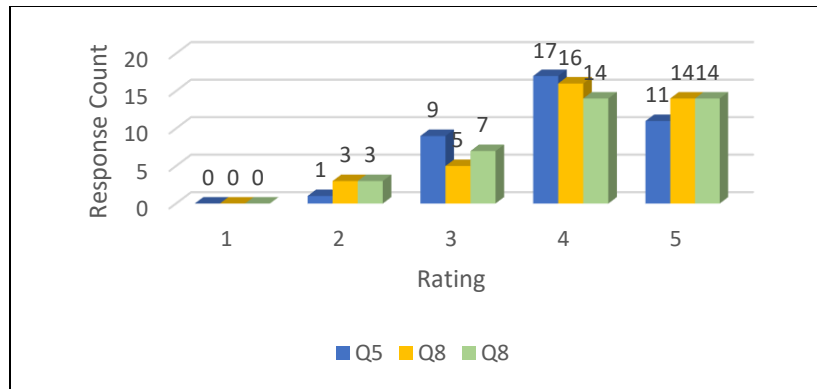


Figure 5.4: Rating on Performance of the Application

- Usefulness

Given that the functionality category has an adequate rating of 3.92, it can be said that for every user who has participated in the UAT process, the system is practical and helpful. Below graph shows overall feedback on usefulness.

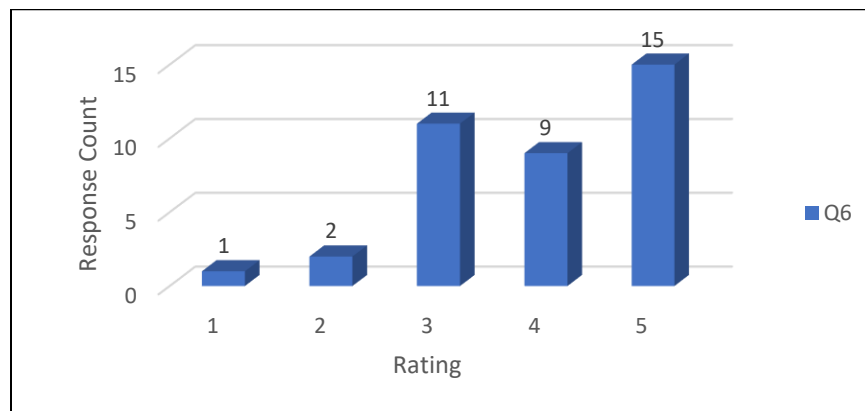
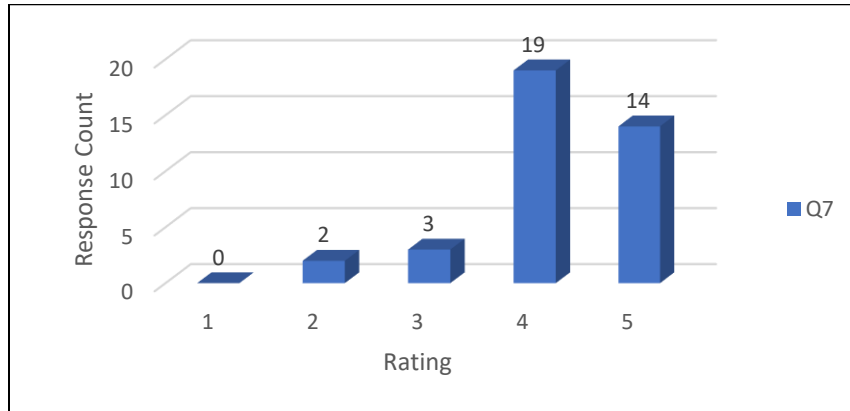


Figure 5.5: Rating on System Usefulness

- Accuracy

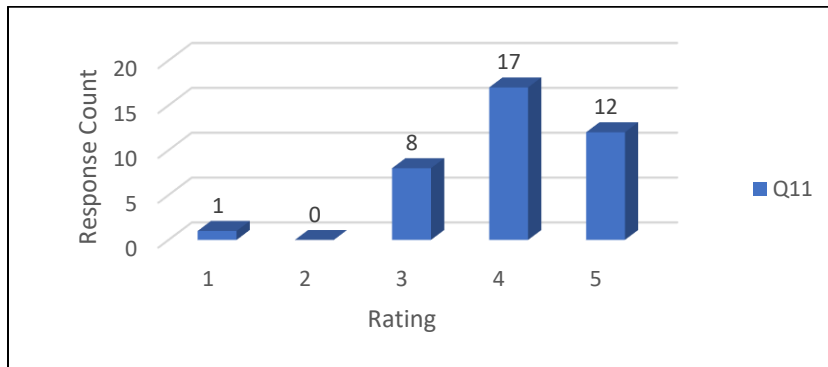
The accuracy category had the highest mean score of all four categories, with a rating of 4.184. Thus, it can be said that for every user who has participated in the UAT process, the system accurate. It means reports and data panel of the system meet the required accuracy level. The overall feedback status shown in the below table.



*Figure 5.6: Rating on System Information accuracy*

- Security

With a security score of 4.03, it indicates that users are satisfied with the system's security measures. It will confirm that the conclusion that the system's overall security for the data and information it stores is quite good. The user rating chart is shown below.



*Figure 5.7: Rating on system security*

- Availability

For the availability category it has received a rating of 3.947 as the mean. Considering the adequate rate, we can say that the user happy with status of system availability status. It will meet the user required level. Below is the overall feedback chart on system availability.

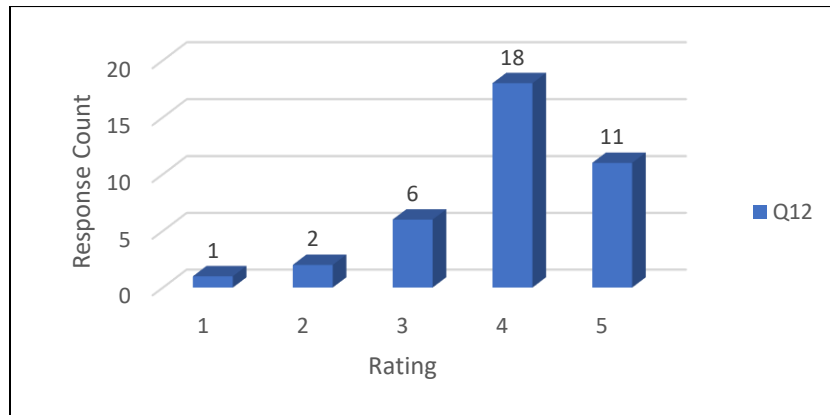


Figure 5.8: Rating on system availability

Therefore, it can be concluded that the system has successfully met the objectives of development, ensuring customer satisfaction. As such, it is recommended for implementation in the production environment. Below are the overall summery of the all responses.

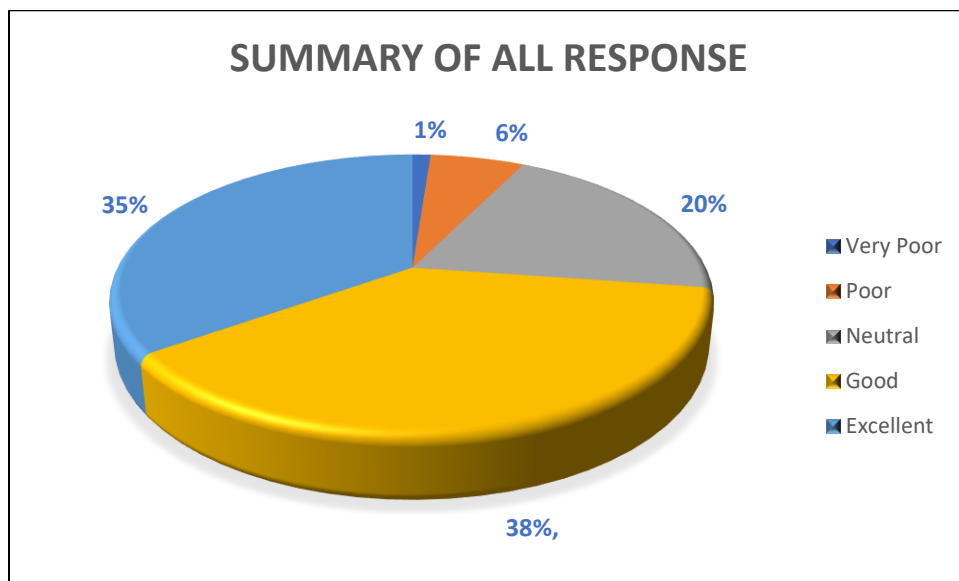


Figure 5.9: Summary of overall user experience

## Chapter 6 – Conclusion

As mentioned in the opening chapter, the primary goal of the project was to automate the Bank of Ceylon's IT department's manual, paper-based procedure by implementing a web-based “Network Firewall and Access Management System”. The suggested solution is to increase the organization's overall effectiveness and sustainability by automating manual operations and enhancing security, transparency, and efficiency. The successfulness of the developed system totally depend on main three aspects.

1. Whether the developed solution can take the place of the current manual procedure and carry it out on a digital platform.
2. Whether the current users are able to use digital platform for their manual task and existing process transferable to the new system.
3. Whether it able to Track the main four functions (firewall port open, Internet request, VA request and the password reset) accurately.

Based on rating earn by the developed Network Firewall and Access Management System from users, It confirmed the new system can override the old manual process. Depend on user ratings for google form, it can be concluded that the users able to manage their manual work in new digital platform.

When designing new automated system, it is very easy to describe the process and designing. Because most of users have IT based knowledge. Most of difficulties such as lot of paper works, security risks, inefficiencies, resource wastage and identifying unnecessary bottle necks that faced by user resolved by the new Network Firewall and Access Management System. It became huge advantage when requirement gathering, user trainings and testing. Because of it related staff developed system can leading to more successful outcomes and higher user satisfaction. Therefore, it can be said that after the system is put into use in a production environment, the transformation can be implemented successfully.

Thus, it can be concluded that the Network Firewall and Access Management System's development and installation were effective and that the goal was met in the allotted time frame.

## **6.1 Future Work**

Even though the Network Firewall and Access Management System has achieved higher user satisfaction, there are opportunities to further enhance its value proposition through the addition of new functionalities.

Suppose to The notifications via Email, Text messages to related user when he/she assign new task. And currently when request VA request internet security ready the environment for scan. Then user have to go physically and put credentials. In next phase user will have option to get remote session through the system and put credential remotely. Network Firewall and Access Management System's owner is internet security team. In future they will have attractive live dash board that showing live status on requests.

When system go live it will be host in VM servers. Later on, the server will be duplicated to the disaster recovery server from the production environment. To move data from the live database to the disaster recovery database, a real-time data replication mechanism will be used.

## List of References

Accusoft Corporation (2023) ‘7 Benefits of Digital Expense Reports With OnTask - OnTask’. Available at: <https://www.ontask.io/blog/7-benefits-of-digital-expense-reports-with-ontask/>.

Architecture, P.M.C. (2021) ‘CodeIgniter Architecture Data flow in CodeIgniter’, *JavaTpoint*, pp. 1–7. Available at: <https://www.javatpoint.com/codeigniter-architecture>.

Bank of Ceylon. (2017) ‘Bank of Ceylon’, *Bank of Ceylon.*, p. 7010. Available at: [https://www.boc.lk/index.php?route=information/information&information\\_id=4](https://www.boc.lk/index.php?route=information/information&information_id=4).

Cision (2023) ‘Accusoft Launches OnTask for Automated Business Workflows’. Available at: <https://www.prnewswire.com/news-releases/accusoft-launches-ontask-for-automated-business-workflows-300415082.html>.

CodeIgniter Foundation (2019) ‘Application Structure — CodeIgniter 4’. Available at: <https://codeigniter4.github.io/userguide/concepts/structure.html>.

Cynotex (2020) ‘Check out the new big things in CodeIgniter 4 - Cynoteck’. Available at: <https://cynoteck.com/blog-post/the-new-big-things-in-codeigniter-4/>.

Hernandez, R.D. (2021) ‘The Model View Controller Pattern – MVC Architecture and Frameworks Explained’, *FreeCodeCamp* [Preprint]. Available at: <https://www.freecodecamp.org/news/the-model-view-controller-pattern-mvc-architecture-and-frameworks-explained/>.

Indeed (2023) ‘What Is Corporate Management and How Does It Work\_ (With Types) \_ Indeed’. Available at: <https://www.indeed.com/career-advice/career-development/corporate-management>.

kissflow (2023a) ‘Features \_ Kissflow Workflow Management Software’. Available at: <https://kissflow.com/workflow/features/>.

kissflow (2023b) ‘Low-Code No-Code Work Platform - Kissflow’. Available at: <https://kissflow.com/>.

Legito (2023a) ‘Administering Users and Permissions’, pp. 1–357. Available at: <https://www.legito.com/knowledge-base/users-and-permissions/>.

Legito (2023b) ‘Ethos & Story \_ Legito’. Available at: <https://www.legito.com/>.

Legito (2023c) ‘Infrastructure \_ Legito’. Available at: <https://www.legito.com/developers/infrastructure/>.

Legito (2023d) ‘Legito Software - 2023 Reviews, Pricing & Demo’. Available at: <https://www.softwareadvice.com.au/software/178279/legito#pricing>.

Lucidchart (2023) ‘Introducing Types of UML Diagrams \_ Lucidchart Blog’. Available at:

<https://www.lucidchart.com/blog/types-of-UML-diagrams>.

Muhammad Abedin et al. (2010) '(PDF) Analysis of firewall policy rules using traffic mining techniques'. Available at: [https://www.researchgate.net/publication/220526786\\_Analysis\\_of\\_firewall\\_policy\\_rules\\_using\\_traffic\\_mining\\_techniques](https://www.researchgate.net/publication/220526786_Analysis_of_firewall_policy_rules_using_traffic_mining_techniques).

Nishadha (2023) 'UML Class Diagram Relationships Explained with Examples \_ Creately'. Available at: <https://creately.com/guides/class-diagram-relationships/>.

OnTask (2023) 'OnTask Software Reviews, Demo & Pricing - 2023'. Available at: OnTask Software Reviews, Demo & Pricing - 2023.

ONTASK (2016) 'Pricing and Plans'. Available at: <https://developer.here.com/plans>.

ONTASK (2023) 'How to Add Email Notifications to a Workflow \_ OnTask'. Available at: <https://www.ontask.io/resources/help-center/email-notifications-in-workflow/>.

Radostin Dimov et al. (2021) '(PDF) Vulnerability Analysis in Server Systems'. Available at: [https://www.researchgate.net/publication/357016883\\_Vulnerability\\_Analysis\\_in\\_Server\\_Systems](https://www.researchgate.net/publication/357016883_Vulnerability_Analysis_in_Server_Systems).

Ravikiran A S (2023) 'ER Diagrams in DBMS\_ Entity Relationship Diagram Model \_ Simplilearn'. Available at: <https://www.simplilearn.com/tutorials/sql-tutorial/er-diagram-in-dbms>.

Software Advice (2023a) 'Buildium Software Reviews & Ratings | 2022 | Software Advice'. Available at: <https://www.softwareadvice.com/property/buildium-property-manager-profile/reviews/>.

Software Advice (2023b) 'Kissflow Software Reviews, Demo & Pricing - 2023'. Available at: <https://www.softwareadvice.com/bpm/kissflow-profile/>.

Sunstein, C.R. (2019) 'Our Own', *Why Nudge?: The Politics of Libertarian Paternalism*, pp. 163–166.

SURABHI, S. (2022) 'CodeIgniter Framework for PHP - An Introduction (Bonus\_ vs Laravel)'. Available at: <https://www.netsolutions.com/insights/codeigniter-framework-features/>.

talend (2023) 'What is MySQL\_ Everything You Need to Know \_ Talend'. Available at: <https://www.talend.com/resources/what-is-mysql/>.

Technologies, O. (2016) 'How to Prevent SQL Injection in PHP', *Http://Www.Wikihow.Com/ [Preprint]*. Available at: <http://www.wikihow.com/Prevent-SQL-Injection-in-PHP>.

Udemy (2023) 'CodeIgniter 4\_ Build a Complete Web Application from Scratch \_ Udemy'. Available at: <https://www.udemy.com/course/codeigniter-from-scratch/>.

VeraCode (2018) 'Guide to CSRF (Cross-Site Request Forgery) | Veracode', *VercaCode [Preprint]*. Available at: <https://www.veracode.com/security/csrf>.



## **Appendix A – MIS Reports**

### **Introduction**

Management Information System (MIS) reports include information which helps higher management to make decisions. It is a kind of system that collect, store, and provide important information to manage business. User can give the criteria to the system and then system will generate the report according to related criteria that user provide. MIS system can process massive amount of data from multiple sources and generate the report. Those MIS report are referred by the higher management to take decisions to run operation smoothly without any bottle necks. MIS reports will update the higher management about the status of the ongoing task. In section describes the MIS report layout and the types of reports generated in the system.

### **Administrative Reports**

Administrative reports will include all the MIS reports related to the user management and day to day user operations handled through the system.

#### **Active users by unit wise**

This report was designed to get the active system users assign to each unit. Higher management able to view list of users with their privileges that assign to each unit by executing this report.


		<b>Network Firewall and Access Management System</b> <b>User List - Unit Wise</b>					
Unit :		ALL		Start Date :		12/1/2023	
				End Date :		12/30/2023	
ID	PF Number	Name	Email	Mobile	Extention	User Role	Registered Date
General Applications	207391	K.D.L.I Lakmal	<a href="mailto:lelumlakmal@boc.lk">lelumlakmal@boc.lk</a>	774856896	13562	Administrator	2023-04-19
Product and Development	232017	R.Diwanika	<a href="mailto:diwanika@boc.lk">diwanika@boc.lk</a>	714585963	3562	User	2021-06-01
Internet Banking	231960	Thilanga Attanayaka	<a href="mailto:thilanga@boc.lk">thilanga@boc.lk</a>	754000456	3523	User	2022-11-30
ATM	207441	Dewa Chinthaka	<a href="mailto:chinthaka@boc.lk">chinthaka@boc.lk</a>	776245789	3548	User	2022-11-30
Report ID - RU100001 / Generated User - K.D.L.I Lakmal (207391) / Date - 2023-11-30							

Figure A.1: User list

If the user selects the unit or date range system will generate the report and it will display the output as shown in the above figure.

#### List of users by user status - Inactive

This report was designed to get the list of system users who are deactivated. Administrators will be able to generate this report by selecting the unit.


		<b>Network Firewall and Access Management System</b> <b>User List - Inactive</b>				
				Start Date :		12/1/2023
				End Date :		12/30/2023
#	PF Number	Name	Unit	User Role	User Status	Last Login
1	207205	L.R.V Fernando	GA	Admin	Inactive	2023-06-14
3	232017	G.M Atapattu	GA	Manager	Inactive	2023-10-15
2	188190	S.M Rinos	GA	EO	Inactive	2023-09-14
Report ID - RU100002 / Generated User - K.D.L.I Lakmal (207391) / Date - 2023-11-29						

Figure A.2: User list Inactive


When user select unit or date range and generate the report, system will generate a report as shown in this figure.

## Firewall, VA and Internet Access Request Module

Firewall request module include report which present the details of pending requests, approved requests, rejected requests and the Vulnerability assessment scan that request by each unit. Most of the reports available in this will access by the senior management and the higher management. Using report of this module higher management able to manage the bottle necks of the process and speed up the authorization process of grant Internet, open ports, and Vulnerability assessment scan.

### Firewall Request Summery Report– Overall Status

Users can generate the summery reports on considering all requests that made by each unit.

		<b>Network Firewall and Access Management System</b> <b>Firewall Access Detail Report</b>							
General Application		Start Date : 12/1/2023 End Date : 12/30/2023							
PF Number	Unit	Requested User	Request Type	Requested Date	Source IP	Destination IP	Protocol	Ports	Status
200240	General Application	K.D.L.I Lakmal	Internet Request	2023-12- 28	172.20.106.159	172.20.8.132	TCP	4446	complete
231960	General Application	Thilanga Attanayaka	Firewall Port Open	2023-12- 30	172.20.8.160	172.20.8.32	UDP	443	pending
231902	General Application	R.T.M.P Senevirathna	VA Request	2023-12- 15	172.20.106.224	172.24.28.114	TCP	50000 442	complete
232017	General Application	R.Diwanika	Firewall Port Open	2023-12- 25	172.20.106.131	172.24.28.113	TCP	433	complete
Report ID - RFA100002 / Generated User - K.D.L.I Lakmal (207391) / Date - 2023-12-30									

*Figure A.3: Firewall Access Detail Report*

In this figure, it shows a summary report which was generated by a team in the Internet Security team on the status of all requests and selected date range.

- Users and senior managers were allowed to generate the report only for the user's unit which was mentioned in the user profile.
- Higher management (AGMs and DGMs) were allowed to select a unit and generate the report.
- Higher management were allowed to generate the report for all the units at once to view the status of the requests of all the units.

### Internet Access – Daily Expiration Report

This report design for the network team. By generating this report, it gives details of Internet access expiration unit wise.

BANK OF CEYLON

Bankers to the Nation

Network Firewall and Access Management System

Internet Access Expiration Report

Unit :All

Start Date :12/1/2023

End Date :12/30/2023

PF No	Mobile	Unit	Date Grant	Expiration Date	Requested User	IP Address	Category	Type	Explanantion	Status
207391	776028309	Genaral Application	2023-12-02	12/3/2023	207391	172.24.28.14	Permanent	Without Proxy	VA Fixing	Complete
203753	778545789	Core Banking Deveolpment	2023-12-01	12/4/2023	231902	172.24.28.113	Temp	With Proxy	Download patch	Pending
207393	758956123	Internet Banking	2023-12-03	12/5/2023	232017	172.20.106.254	Permanent	Full	Update OS	Complete


Report ID - RI100101 / Generated User - K.D.L.I Lakmal (207391) / Date - 2024-01-01

*Figure A.4: Internet Access Expiration Report*

This figure shows an internet access expiration report which was generated by a team in the Network team on the status of internet access requests. The network team can use this report to remove internet access from expired PC's.

## Vulnerability Assessment Request Report– Overall Status

This report uses by the internet security team to manage VA requests. It represents the VA request raised by each team with the details of the server.

 BANK OF CEYLON Bankers to the Nation		<b>Network Firewall and Access Management System</b> <b>Vulnerability Assesment Request Report</b>							
Unit :		All		Start Date		12/1/2023			
				End Date :		1/30/2024			
PF No	Unit	Email	Mobile	Extention	Date	OS	Server IP	Explanation	Status
207391	Genaral Application	<a href="mailto:lelumlakmal@boc.lk">lelumlakmal@boc.lk</a>	776028309	13562	12/1/2023	Linux	172.20.28.160	Critical Live server	Complete
177198	PM	<a href="mailto:sashika@boc.lk">sashika@boc.lk</a>	717051802	3523	12/5/2023	Windows	172.24.28.113	UAT Server	Pending
231902	Genaral Application	<a href="mailto:madushi@boc.lk">madushi@boc.lk</a>	778545789	3562	1/5/2024	Linux	172.24.28.132	Production Server	Complete
203753	Core Bank Development	<a href="mailto:Gehan@boc.lk">Gehan@boc.lk</a>	778545789	3573	1/10/2024	Linux	172.20.70.8	DR Server	Pending
Report ID - RVA100001 / Generated User - K.D.L.I Lakmal (207391) / Date - 2024-01-30									

*Figure A.5: Vulnerability Assessment Request Report*

It shows a Vulnerability Assessment Request report with its status. Internet security team members can generate report by selecting date range and if they want, they can generate same report unit wise.

## AD Password Maintenance Module

AD Password maintenance module include report that represent the details that made by branch users, head office users and intern trainees to create and reset AD passwords. Management able to see pending password create/reset requests, approved requests, and rejected requests. Using this report, senior management of technical department can easily handle the bunch of requests that they are getting all over the country. They can schedule the requests efficient way by using this report. Using AD password maintenance detail report of this module higher management able to manage the bottle necks of the process and speed up the process manage AD password.

## AD Password Maintenance Detail Report– Overall Status

Technical department can generate the AD password maintenance reports on considering all requests that made by each branch and each unit.

BANK OF CEYLON

Bankers to the Nation

Network Firewall and Access Management System

AD Password Maintenance Detail Report

Unit :All

Start Date :12/1/2023

End Date :12/30/2023

PF No	Branch	Requested User	Email	Extension	Mobile	NIC	Requested Date	Branch Code	Status
207391	Head Office	K.D.L.I Lakmal	K.D.L.I Lakmal	13562	776028309	198904300511	2023-12- 02	3230	complete
231960	Head Office	Thilanga Attanayaka	Thilanga Attanayaka	3523	754578258	199707900411	2023-12- 10	3231	pending
231902	Head Office	R.T.M.P Senevirathna	R.T.M.P Senevirathna	3562	778545789	199704550455	2023-12- 15	3232	complete
207393	Head Office	S. Jayakodi	S. Jayakodi	3558	758956123	198802300345	2023-12- 25	3233	complete

Report ID - RPWD100002 / Generated User - K.D.L.I Lakmal (207391) / Date - 2024-01-01

*Figure A.6: AD Password Maintenance Detail Report*

If the technical user selects the unit/branch or date range system will generate the report and it will display the output as shown in this figure.

## Appendix B – Test Plan

Given below are the additional test cases used for the testing of this system.



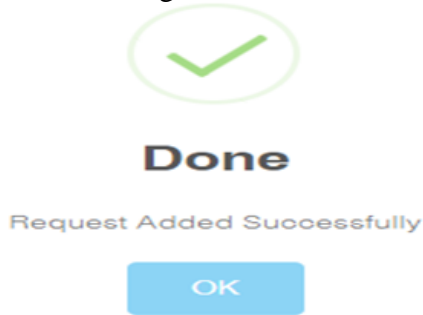
ID	Activity	Test Case Steps	Expected Result
3.1	Add New VA Request	Click the menu option “VA Request” under the “Add request”.	Add VA Request form will disappear to the user
3.2	Check Validations	Server IP Cannot be empty	Should display an error message if validation fails.  Select OS  The OS field is required.  Select Criticality Level  The Criticality field is required.
		Select OS	
		Select Criticality Level	
3.3	Successfully add VA request	After input all required fields Press request button.	Confirmation Message  

Table B.11:VA request test case

- Test Cases for add new firewall port open request

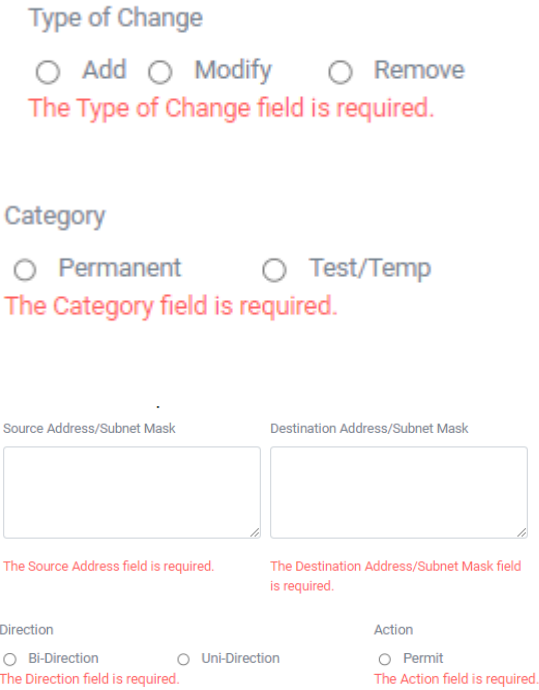
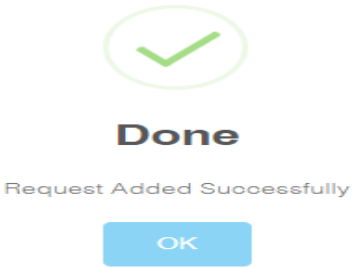
ID	Activity	Test Case Steps	Expected Result
4.1	Create New Firewall Request	Click the menu option “Add firewall Request“ under the “Add request”.	Add Firewall Request form will disappear to the user
4.2	Validation On input fields	<div>Type of change must be select.</div> <div>Category must be select</div> <div>Source Address cannot be empty.</div> <div>Designation Address cannot be empty.</div> <div>Protocols cannot be empty</div> <div>Direction must be select</div> <div>Action must be select</div>	 <p>Type of Change</p> <p><input type="radio"/> Add <input type="radio"/> Modify <input type="radio"/> Remove</p> <p>The Type of Change field is required.</p> <p>Category</p> <p><input type="radio"/> Permanent <input type="radio"/> Test/Temp</p> <p>The Category field is required.</p> <p>Source Address/Subnet Mask</p> <p>Destination Address/Subnet Mask</p> <p>The Source Address field is required. The Destination Address/Subnet Mask field is required.</p> <p>Direction</p> <p><input type="radio"/> Bi-Direction <input type="radio"/> Uni-Direction</p> <p>The Direction field is required.</p> <p>Action</p> <p><input type="radio"/> Permit</p> <p>The Action field is required.</p>
4.3	Successfully add firewall request	After input all required fields Press request button.	<p>Request will be added to database successfully.</p>  <p>Done</p> <p>Request Added Successfully</p> <p>OK</p>

Table B.12: Test case for firewall port open request




ID	Activity	Test Case Steps	Expected Result																																	
5.1	Create New Role (Add)	Go to Role Management and click on Add, Add the user role name	After adding the role name correctly, the role name can be seen in the table below. When it returns a validation error user role will not be created successfully.																																	
5.2	Edit Role	Click on record need to edit, in the relevant column and enter the correct name.	New role name is appearing in the relevant column  Role Name  Manager																																	
5.3	Role Module Assignment	Select the relevant role name on the give drop down.	Assigned modules will be appeared. <table><thead><tr><th>Permission Name</th><th>ch val</th><th>Action</th></tr></thead><tbody><tr><td>AUTH_app</td><td>1</td><td><input checked="" type="checkbox"/></td></tr><tr><td>AUTH_req</td><td>0</td><td><input type="checkbox"/></td></tr><tr><td>FR_add</td><td>1</td><td><input checked="" type="checkbox"/></td></tr><tr><td>FR_app</td><td>0</td><td><input type="checkbox"/></td></tr><tr><td>FR_can</td><td>1</td><td><input checked="" type="checkbox"/></td></tr><tr><td>FR_edt</td><td>1</td><td><input checked="" type="checkbox"/></td></tr><tr><td>RM_add</td><td>1</td><td><input checked="" type="checkbox"/></td></tr><tr><td>ST_app</td><td>1</td><td><input checked="" type="checkbox"/></td></tr><tr><td>ST_pend</td><td>1</td><td><input checked="" type="checkbox"/></td></tr><tr><td>VA_add</td><td>1</td><td><input checked="" type="checkbox"/></td></tr></tbody></table>	Permission Name	ch val	Action	AUTH_app	1	<input checked="" type="checkbox"/>	AUTH_req	0	<input type="checkbox"/>	FR_add	1	<input checked="" type="checkbox"/>	FR_app	0	<input type="checkbox"/>	FR_can	1	<input checked="" type="checkbox"/>	FR_edt	1	<input checked="" type="checkbox"/>	RM_add	1	<input checked="" type="checkbox"/>	ST_app	1	<input checked="" type="checkbox"/>	ST_pend	1	<input checked="" type="checkbox"/>	VA_add	1	<input checked="" type="checkbox"/>
Permission Name	ch val	Action																																		
AUTH_app	1	<input checked="" type="checkbox"/>																																		
AUTH_req	0	<input type="checkbox"/>																																		
FR_add	1	<input checked="" type="checkbox"/>																																		
FR_app	0	<input type="checkbox"/>																																		
FR_can	1	<input checked="" type="checkbox"/>																																		
FR_edt	1	<input checked="" type="checkbox"/>																																		
RM_add	1	<input checked="" type="checkbox"/>																																		
ST_app	1	<input checked="" type="checkbox"/>																																		
ST_pend	1	<input checked="" type="checkbox"/>																																		
VA_add	1	<input checked="" type="checkbox"/>																																		
5.4	Change Role's Assigned Modules	Tick or Untick on the checkbox	Permission will be updated successfully.   <b>Permission Added Successfully !</b>  OK																																	

Table B.13: Test case for user role

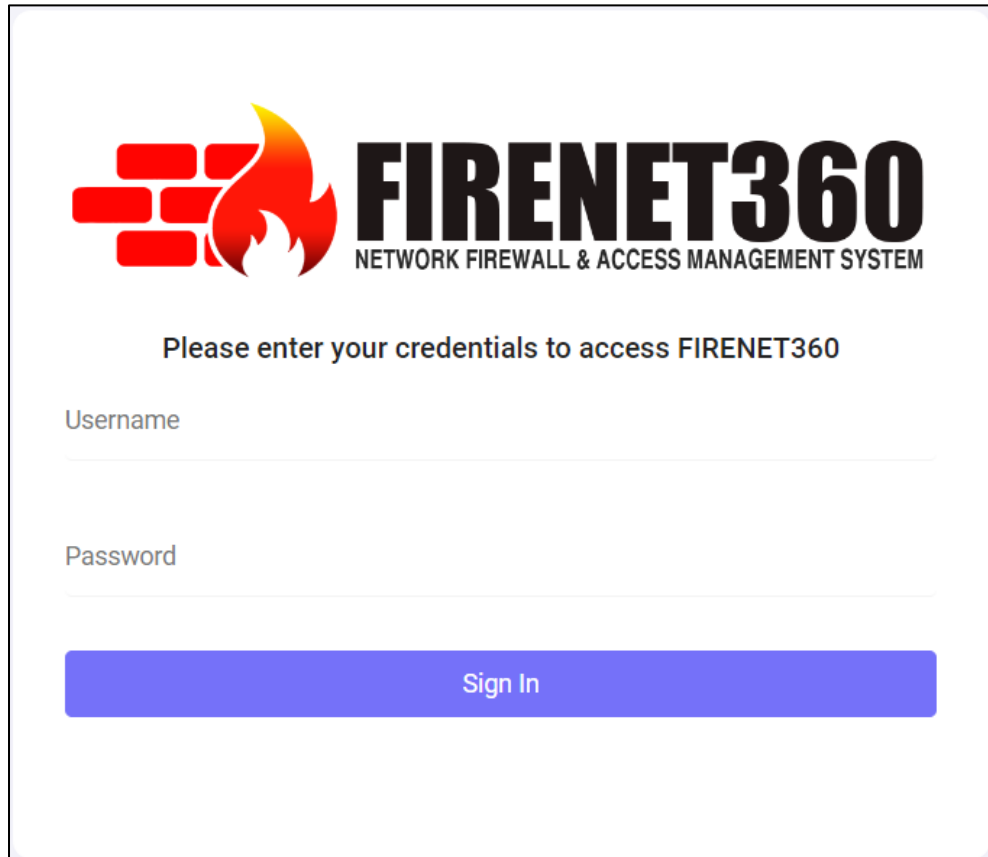
<b>Test ID</b>	<b>Description</b>	<b>Pass / Fail</b>
3.1	Add New VA Request	Pass
3.2	Check Validations	Pass
3.3	Successfully add VA request	Pass
4.1	Create New Firewall Request	Pass
4.2	Validation On input fields	Pass
4.3	Successfully add firewall request	Pass
5.1	Create New Role (Add)	Pass
5.2	Edit Role	Pass
5.3	Role Module Assignment	Pass
5.4	Change Role's Assigned Modules	Pass

*Table B.14: Status of test cases*

## Appendix C – User Manual

This part contains the user manual for the produced system, which includes screenshots and usage instructions for the key capabilities.

### Login



*Figure C.7: User Login*

- Above figure shows the initial screen of the developed system. User able to put credentials to inputs on screen. Registered active user able to login to the system using correct credentials.
- This screen contains the validations for user inputs. User should input both username and password to the input field. System will authenticate users and the users who get successful authentication able to redirect to the home page. Users who enter invalid credentials or Disable users get error message.

- The user's account will automatically lock after more than three incorrect password entries. The account cannot be reactivated by anybody other than an administrator.

## Home Panel

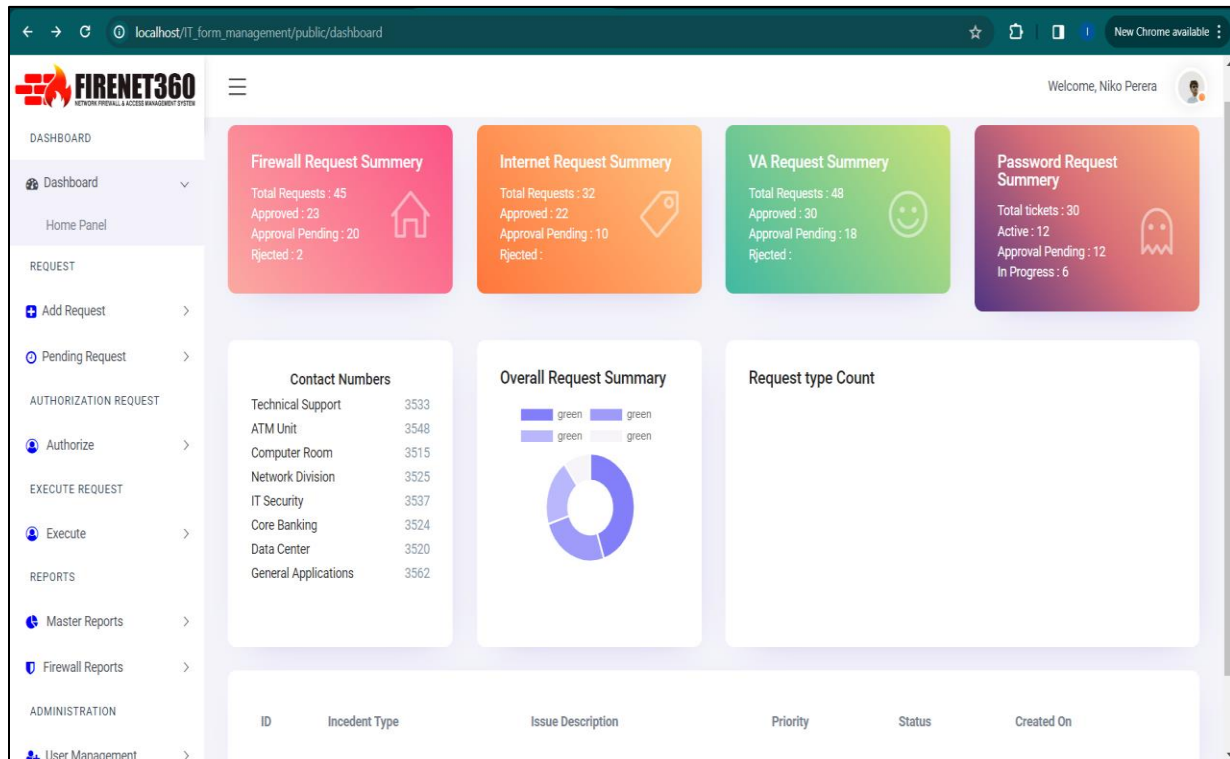


Figure C.8: User Dashboard

- After successful login user is able to access above dashboard.
- Above figure represents the dashboard which contains the summary of each user.
- Each user can easily review the request detail summary and bottom of the page there is table which contains the pending requests according to the user. By clicking the item user must be able to see request details in read only manner.

## Firewall port open request Function

**FIRENET360** NETWORK FIREWALL & ACCESS MANAGEMENT SYSTEM

Welcome, Niko Perera

**Requestor's Information**

Department: IT Division Designation: EO Requester: Ielum

PF No: 207391 Email: lelumiakmal@boc.lk Mobile No: 0776028309

Extension Number: 13562 Date: 2024-03-05

**Information about the access request**

Type of Change: ☐ Add ☐ Modify ☐ Remove Category: ☐ Permanent ☐ Test/Temp

The Type of Change field is required. The Category field is required.

Effective From: 2024-03-05 Expiration Date: 2024-03-05

Explanation of Change Application

**Detailed Firewall Request Information**

Source Address/Subnet Mask: Destination Address/Subnet Mask: Protocols: Ports:

The Source Address field is required. The Destination Address/Subnet Mask field is required. The Protocols field is required. The Ports field is required.

Direction: ☐ Bi-Direction ☐ Uni-Direction Action: ☐ Permit ☐ Deny

The Direction field is required. The Action field is required.

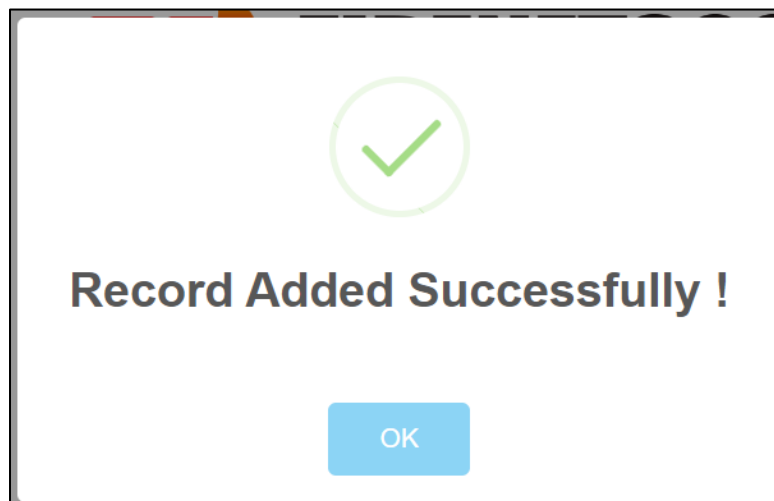
**Request**

Copyright © Designed & Developed by General Application Unit 2023

*Figure C.9: Firewall port open request function*

- In above form, it will facilitate the user to request, firewall port open request. As a first step user login to the system and fill the firewall port details to the above form.

- This function will be available for all users. The grade with Executive officers to the higher management.
- As shown above form will guide user to fill the data with correct details. It contain the validations for empty fields and incorrect inputs. When the page is loaded, user details will be automatically filled. They are only read only values. So it automatically prevents the incorrect inputs and request will track against the user. All requests made by the system will record against the login user.
- After completing the firewall port information, user submits the form for manager approval by clicking Request button.
- After the record has been successfully added to the database, a confirmation message will appear as below.



*Figure C.10: Successful request*

- Similar to the firewall port open request module, Internet request module and VA request module has same process to add request. Only different is the bottom section of some fields are different according to the module. Automatically user (requester) data filling function will be available for all forms.

- These three functions will also be available for all users. The grade with Executive officers to the higher management.
- After adding data successful message will be appear same as firewall port open request module.
- Request will be send to the related chief manager for approval.

## **VA request Function**

By clicking menu option VA request under add request, it will display the following page.

The screenshot displays the FIRENET360 web application interface for the VA Request Function. The interface is divided into a sidebar and a main content area. The sidebar on the left contains navigation links: DASHBOARD, REQUEST, Add Request (with a dropdown), Pending Request, AUTHORIZATION REQUEST, and EXECUTE REQUEST. The main content area is titled 'Requestor's Information' and contains several input fields: Department (IT Division), Position (EO), Requester (Ielum), PF No (207391), Email (IelumIakmal@boc.lk), Mobile No (0776028309), Ext (13562), and Date (2024-02-15). Below this is the 'Information about the Server' section with fields for Server Os (Windows), Server IP, and Server Criticality (High). A 'Request' button is located at the bottom right of the form. The footer of the page indicates 'Copyright © Designed & Developed by General Application Unit 2023'.

*Figure C.11: VA Request Function*

- Add validations for server details fields.
- Click on request will send VA request to the related chief manager.

## **Internet request Function**

By clicking menu option Internet request under add request, it will display the following page.

The screenshot displays the FIRENET360 web application interface for the Internet Request Function. The interface is structured with a sidebar menu on the left, a main content area, and a footer. The sidebar menu includes sections for DASHBOARD, REQUEST, AUTHORIZATION REQUEST, EXECUTE REQUEST, REPORTS, and ADMINISTRATION. The main content area is titled 'Requestor's Information' and contains several form fields: Department (IT Division), Position (EO), Requester (Ielum), PF No (207391), Mobile No (0776028309), Email (Ielumlakmal@boc.lk), Ext (13562), and Date (2024-03-06). Below this is the 'Information about the PC' section with fields for IP Address, Access Type (With Proxy), Category (Permanent/Temp), IP Address Required, Effective From (2017-06-03), and Expiration Date (2017-06-03). A 'Request' button is located at the bottom right of the form.

*Figure C.12: Internet Request Function*

- Same as above Add request function. Validation added to the fields on the pc information's.
- Click on request will send Internet request to the related chief manager.



## **Password create/reset function**

By clicking menu option Password request under add request, it will display the following page.

The screenshot shows the FIRENET360 web interface. The left sidebar contains a menu with options like Dashboard, Add Request, Pending Request, and Execute. The main content area is titled 'Request Type Information' and 'Staff Member Information'. The 'Request Type Information' section has radio buttons for 'Create New User' and 'Reset Password', and a 'Reason to reset' section with options 'Forgotten' and 'Account is disabled'. The 'Staff Member Information' section includes fields for 'Name with initials', 'Full Name', 'Last Name', 'Grade', 'PF No', 'Mobile No', 'Email', and 'Ext'. A 'Request' button is at the bottom right.

*Figure C.13: Password create/reset function*

- Password create/reset module bit different from other modules. In this form requester fill other user information's. Above three models login user information automatically generate as the requester.
- There is two type of users.one is permanent staff members and other one is probation interns. One request only can have permanent staff or intern staff member. One request can't have both. Form have validation to handle it.
- Click on request will send Internet request to the related chief manager.

## Unit Manager Approval function

- By clicking menu option pending firewall request under pending request, it will display the following panel with detail of pending firewall port open requests that related to the login user.

Firewall Requests

Show 10 entries

Search:

Req_ID	Name	PF Number	Email	Mobile	Status	Action
3	samudadw	Test	Test	213	Approved	
4	samudadwwww	Test	Test	213	Approved	
5	samudadwwww323	Test	Test	213	Approved	
6	samudadwwww323wew	Test	Test	213	Approved	
11	lakmal	test	lelumlakmal@boc.lk	776028309	Approved	
14	samuda	test	lelumlakmal@boc.lk	776028309	Approved	
18	Lelum	207391	b.akalanika@gmail.com	776028309	Approved	
19	lakmal check 09 21	207391	lelumlakmal@gmail.com	2147483647	Approved	
25	Gehan		madushi@boc.lk	776028309	Approved	
26	Gehan		lelumlakmal@boc.lk	776028309	Approved	

Showing 1 to 10 of 13 entries

Previous 1 2 Next

*Figure C.14: Unit Manager Approval*

- Pending firewall request function is only available for users in chief manager grade.
- Manager is able to approve firewall port open request by approved button.
- If manager want to see more details on the selected row, by clicking edit icon user will be able to see more details.
- Related login manager will automatically load to the page as below figure. Manager can check the detail and approve. Manager able to put comment in this option. But manager can't edit the other fields.
- Manager able to check the details and approve or reject the request. After manager approved it sends the Internet security division to authorize the request.
- More details page of pending request appear as follows.

### Requested Firewall Information

Name

Gehan

Email

lelumiakmal@boc.lk

Mobile No

776028309

Ext

3562

Date

2024-02-22

PF No

177856

Department

IT

Position

2

### Information about the access request

Type of Change

☒ Add
☐ Modify
☐ Remove

Category

☒ Permanent
☐ Test/Temp

Expiration Date

Invalid date

Effective From

0000-00-00

Explanation of Change Application

### Detailed Firewall Request Information

Source Address/Subnet Mask

172.20.106.159

Destination Address/Subnet Mask

172.24.28.32

Protocols

TCP

Ports

443  
50000

Direction

☐ Bi-Direction
☒ Uni-Direction

Action

☒ Permit
☐ Deny

Comment

please do it ASAP

Approved By

Rinos

Reject

Approve

Figure C.15: More details of Pending Approvals

- Other three function also have same functions as the Pending Firewall Request list panel.
- Manager able to get list of pending requests for each of function separately. Same as above manager able to view more detail by selecting one record.
- Below are the related pending request list panel for each function.

## Panel for Pending Internet request for approval

The screenshot shows the FIRENET360 web application interface. The sidebar on the left contains the following menu items: DASHBOARD, Dashboard, REQUEST, Add Request, Pending Request (expanded), Pending Firewall Request, Pending Internet Request (selected), Pending VA Request, Pending Password Reset, AUTHORIZATION REQUEST, Authorize, EXECUTE REQUEST, Execute, REPORTS, and Master Reports. The main content area is titled 'Pending Internet Requests' and shows a table with one entry. The table has columns: PF Number, Name, Unit, Email, Mobile, IP Address, Access Type, Effective From, Expire Date, purpose, Status, and Action. The entry has PF Number 207391, Name 1, Unit 1, Email lelumlakmal@boc.lk, Mobile 776028309, IP Address 172.20.106.159, Access Type Without Proxy, Effective From 2024-02-25, Expire Date 2024-02-29, purpose VA Fixing, Status 0, and Action Pending. Below the table, it says 'Showing 1 to 1 of 1 entries' and has 'Previous', '1', and 'Next' buttons. A 'Request' button is also present.

PF Number	Name	Unit	Email	Mobile	IP Address	Access Type	Effective From	Expire Date	purpose	Status	Action
207391	1	1	lelumlakmal@boc.lk	776028309	172.20.106.159	Without Proxy	2024-02-25	2024-02-29	VA Fixing	0	Pending

Figure C.16: Panel for Pending Internet request for approval





















- Have same function as pending firewall request panel.
- Approval function only accessible for manager or above users in the IT department.

## **Panel for Pending VA request for approval**

Pending VA Requests

Show 10 entries

Search:

Req_ID	Name	PF Number	Email	Mobile	Status	Action
3	samudadw	Test	Test	213	Approved	 
4	samudadwwwww	Test	Test	213	Approved	 
5	samudadwwwww323	Test	Test	213	Approved	 
6	samudadwwwww323wew	Test	Test	213	Approved	 
11	lakmal	test	lelumlakmal@boc.lk	776028309	Approved	 
14	samuda	test	lelumlakmal@boc.lk	776028309	Approved	 
18	Lelum	207391	b.akalanka@gmail.com	776028309	Approved	 
19	lakmal check 09 21	207391	lelumlakmal@gmail.com	2147483647	Approved	 
25	Gehan		madushi@boc.lk	776028309	Approved	 
26	Gehan		lelumlakmal@boc.lk	776028309	Approved	 

Showing 1 to 10 of 13 entries

Previous12Next

Figure C.17: Panel for Pending VA request for approval

















- Have same function as pending firewall request panel

## **Panel for Pending password request for approval**

Pending Password Requests

Show 10 entries

Search:

Req_ID	Name	PF Number	Email	Mobile	Status	Action
23			madushi@boc.lk	0	Approved	 
24			madushi@boc.lk	0	Approved	 
25	Gehan		madushi@boc.lk	776028309	Approved	 
26	Gehan		lelumlakmal@boc.lk	776028309	Approved	 
27	Rinos		lelumlakmal@boc.lk	776028309	Approved	 
28	Ielum		lelumlakmal@boc.lk	776028309	Approved	 
29	Ielum	207391	lelumlakmal@boc.lk	776028309	Approved	 
30	Gehan	207361	innovlab@boc.lk	717051802	Approved	 

Showing 11 to 18 of 18 entries

Previous12Next

Figure C.18: Panel for Pending password request for approval

- Have same function as pending firewall request panel

## Authorization Function

WELCOME, NIKO PERERA

Dashboard > Home

### Pending Firewall Request For Approval

Show 10 entries

Search:

Req_ID	Name	PF Number	Email	Mobile	Status	Action
2	samuda	Test	Test	213	Pending	<a href="#">Edit</a> <a href="#">Delete</a>
10	check on 22_4	Test	Test	213	Pending	<a href="#">Edit</a> <a href="#">Delete</a>
29	Ielum	207391	IelumIakmal@boc.lk	776028309	Pending	<a href="#">Edit</a> <a href="#">Delete</a>
30	Gehan	207361	innovlab@boc.lk	717051802	Pending	<a href="#">Edit</a> <a href="#">Delete</a>

Showing 1 to 4 of 4 entries

Previous 1 Next

Copyright © Designed & Developed by General Application Unit 2023

Figure C.19: Authorization Function

- Once manager approve the requests, it will go to the next level.
- Approved firewall request and Internet requests come to the internet security unit to next level approval.
- With the search text box located on top of the table users are able to search record using name or unit.
- If want further details, user can press the action button and application will be displayed the details of selected row.
- As shown in figure C.19 authorization function only accessible for manager or above users in the internet security department only.
- For the pending Internet security function have same function with same design.
- Below figure C.20 contain the form that shows the more details of selected record.

Requestor's Information

Name

lelum

Email

leumlakmal@boc.lk

Mobile No

Ext

Date

PF No

776028309

3562

2024-02-23

207391

Department

Position

1

1

Information about the access request

Type of Change

☐ Add

☒ Permanent

☐ Modify

☐ Remove

Expiration Date

2024-02-27

Effective From

Explanation of Change Application

2024-02-05

Detailed Firewall Request Information

Source Address/Subnet Mask

Destination Address/Subnet Mask

Protocols

Ports

172.20.106.159

172.20.8.32

TCP

443  
50000

Direction

Action

Choose...

Choose...

Authorization from IT Security

Comments From IT Security

Approval of IT Security Unit

Deployment of Firewall Rule

Type of Change

Approval of IT Security Unit

Comments

☒ Yes

☐ No

Approve









Reject

Figure C.20: More details of selected record of a pending Approval

- Manager from security department able to check the detail and approve by putting security comment. After approval it will go the network department to apply the rule.

### **Execute Function**

- Same as above Authorization function after the approvals request End with this stage.

Pending Firewall Requests to Apply						
Show 10 entries			Search: 07			
Req_ID	Name	PF Number	Email	Mobile	Status	Action
18	Lelum	207391	b.akalanka@gmail.com	776028309	Approve	 
19	lakmal check 09 21	207391	leumlakmal@gmail.com	2147483647	Approve	 
29	lelum	207391	leumlakmal@boc.lk	776028309	Approve	 
30	Gehan	207361	innovlab@boc.lk	717051802	Approve	 

Showing 1 to 4 of 4 entries (filtered from 18 total entries)

Previous 1 Next

*Figure C.21: Execute Function*

- Execute function only accessible for manager or above users in the network unit only.
- Once internet security department approve the firewall port open request, the request will be sent to the execute panel.
- Same as the Authorization function network team able to view more detail by selecting a record and apply the rule and update the final status of the request.
- This is the final state that the entire process will come to end.



Following figure contain the list of Internet request list that approved by the internet security team.

Pending Internet Requests to Apply											
✕											
Show 10 entries						Search:					
PF Number	Name	Unit	Email	Mobile	IP Address	Access Type	Effective From	Expire Date	purpose	Status	Action
207391	1	1	lelumlakmal@boc.lk	776028309	172.20.106.159	Without Proxy	2024-02-25	2024-02-29	VA Fixing	0	Pending
Showing 1 to 1 of 1 entries										Previous 1 Next	

Figure C.22: Pending Internet Requests

- Same as the above firewall port open request, the network team check the detail and apply the rule.
- In internet request process, this is the final state that the entire process will come to end.

Following figure contain the list of VA request list that approved by the unit manager.









Pending VA Requests to Execute						
Show 10 entries				Search: 07		
Req_ID	Name	PF Number	Email	Mobile	Status	Action
18	Lelum	207391	b.akalanka@gmail.com	776028309	Approved	 
19	lakmal check 09 21	207391	lelumlakmal@gmail.com	2147483647	Approved	 
29	lelum	207391	lelumlakmal@boc.lk	776028309	Approved	 
30	Gehan	207361	innovlab@boc.lk	717051802	Approved	 
Showing 1 to 4 of 4 entries (filtered from 18 total entries)						Previous 1 Next

Figure C.23 Pending VA Requests

- Same as the above firewall port open request, the internet security team check the detail of request and conduct the VA assessment for requested server.
- When the AV assessment complete the VA, report attach against the request to reference.
- In internet request process, this is the final state that the entire process will come to end.

Following figure C.24 contain the list of password create/reset request list that approved by the unit manager.

Pending Password Requests						
Show 10 entries			Search: Tes			
Req_ID	Name	PF Number	Email	Mobile	Action	
4	samudadwwwww	Test	Test	213	Approve	
5	samudadwwwww323	Test	Test	213	Approve	
6	samudadwwwww323wew	Test	Test	213	Approve	
11	lakmal	test	lelumlakmal@boc.lk	776028309	Approve	
14	samuda	test	lelumlakmal@boc.lk	776028309	Approve	
Showing 1 to 5 of 5 entries (filtered from 18 total entries)					Previous	1 Next

*Figure C.24: Pending password/reset*

- Technical team check the request list and do the required task.
- After complete the task they update the status

## Administrative Function

The screenshot shows the FIRENET360 web application interface. The top header includes the logo, a hamburger menu, and a welcome message for 'Niko Perera'. The left sidebar contains a navigation menu with categories: DASHBOARD, REQUEST, AUTHORIZATION REQUEST, EXECUTE REQUEST, REPORTS, and ADMINISTRATION. The 'ADMINISTRATION' section is expanded, showing 'User Management'. The main content area displays a 'User Information' form with the following fields: First Name, Last Name, PF No, Email, Address, Address 2, City, State (a dropdown menu), and Zip. A 'Submit' button is located at the bottom right of the form. The footer contains a copyright notice: 'Copyright © Designed & Developed by General Application Unit 2023'.

**FIRENET360**  
NETWORK FIREWALL & ACCESS MANAGEMENT SYSTEM

Welcome, Niko Perera

Dashboard > Home

**User Information**

First Name:

Last Name:

PF No:

Email:

Address:

Address 2:

City:

State:

Zip:

**Submit**

Copyright © Designed & Developed by General Application Unit 2023

*Figure C.25: Administrative Function*

- Figure C.25 shows the interface that use to add user.
- User add function only available for admin users only.
- When adding user there will be validation for empty fields, incorrect inputs and email.
- After entering needed data click submit button to the add user to data base.
- After successful adding, user will notify by the confirmation message as follows.

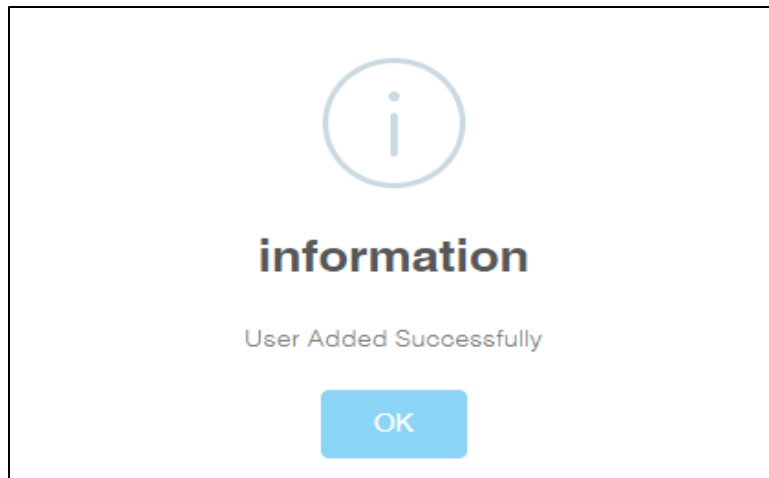


Figure C.26: User module successful notification

- By Clicking on the Edit under user management, it will allow the user to edit the details as shown in below figure C.27.

**User List**

Show 10 entries Search:

First Name	Last Name	PF Number	Email	Mobile	Extension	Registered Date	Status	Action
Gehan	Atapattu	it203753	gehanatapattu@boc.lk	0776547852	3573	1	Active	
Ielum	Lakmal	it207391			13562	1	Active	
Rangika	Fernando	203761	rangika@boc.lk	0774856896	3579	1	Active	
Rinos	S M	177479	rinos@boc.lk		13518	1	Active	
Sashika	Gurusinghe	177198	sashika@boc.lk		3523	1	Active	

Showing 1 to 5 of 5 entries Previous 1 Next

Figure C.27: User List

- User Edit function is only available for admin users only.
- Users are able to select record from the list and by clicking edit button, user details will load to the edit window.
- Using edit window user can edit the user data and update the record.

## Role group function

### Add User Role

Add Role

Show 10 entries

Search:

Role_ID	Role Name	Action
1	EO	
2	Manager	
3	Chief Manager	
4	Intern	
5	trainee	
6	traineeeee	
7	Managerrr	
8	EO 2	
10	AM	

Figure C.28: Role group function

- Using this interface user able to crate user roles.
- User can input the name to the role name field and click Add role button to add record.
- Role name field is validated to the empty string.
- After successful adding, the added user role listed in the below data table.
- Add role group function only available for admin users only.



Role Module Assignment

User Roles Type

EO

loadselected

Show 10 entries

Search:

Permission Name	ch val	Action
AUTH_app	1	<input checked="" type="checkbox"/>
AUTH_rej	0	<input type="checkbox"/>
FR_add	1	<input checked="" type="checkbox"/>
FR_app	0	<input type="checkbox"/>
FR_can	1	<input checked="" type="checkbox"/>
FR_edt	1	<input checked="" type="checkbox"/>
RM_add	1	<input checked="" type="checkbox"/>
ST_app	1	<input checked="" type="checkbox"/>

Figure C.30: Role Module Assignment

- Using above figure user able to give permission to the selected role group.
- In this figure page names are display in the given data table.
- User can add page permission to each user role by adding or removing tick.
- Role model function only available for admin users only.