BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SCIENCE AND ENGINEERING DEPARTMENT

OF COMPUTER SCIENCE



SCIENTIFIC & INDUSTRIAL RESEARCH AND DEVELOPMENT CENTER (SIRDC) SECURE NETWORK

BY

METHOD NDEYA B221451B

RESEARCH PROJECT

A research project proposal submitted in partial fulfillment of the requirements for the Bachelor of Science Honours Degree in Network Engineering.

APPROVAL FORM

The undersigned certify that they have supervised Method Ndeya's (B221451B) dissertation entitled ―Scientific & Industrial Research and Development Center (SIRDC) Secure Network‖ submitted in partial fulfilment of the requirements for the Bachelor of Science Honours Degree in Network Engineering.

Student: …… ……

Date: ……23/06/2026……

Supervisor MR Chituma: ……

Date: ……23/06/2026……

Chairperson Mr Chaka: …… ……

Date: ……23/06/2026……



Dedication

I dedicate this work to my family and friends for their constant support and motivation throughout my academic journey. Finally, this work is dedicated to the pursuit of innovation in network security, with the hope that it contributes to protecting vital research and fostering technological advancement in our society.

Acknowledgement

I would like to express my sincere gratitude to Bindura University of Science Education for the opportunity to undertake this research, which has allowed me to bridge the gap between theoretical knowledge and practical application. I am deeply thankful to my lecturers and especially my academic supervisor, whose guidance, expertise, and encouragement were instrumental in the successful completion of this dissertation.

I also extend my heartfelt appreciation to my industrial supervisor and the management team at the Scientific and Industrial Research and Development Centre (SIRDC). Their mentorship, professional insights, and continuous support during my time with the organization significantly enhanced my understanding of complex network security operations and real-world engineering challenges.

Furthermore, I am grateful to the entire staff at SIRDC for providing a collaborative and conducive environment that facilitated my research and learning.

Finally, I acknowledge my family and friends for their unwavering support, motivation, and encouragement throughout my academic journey. Their belief in me has been a constant source of strength.

Abstract

This project focused on the design and implementation of a secure network infrastructure for the Scientific and Industrial Research and Development Center (SIRDC) using a firewall-based security architecture. The study aimed to improve network security by implementing firewalls, Intrusion Prevention Systems (IPS), Virtual Private Networks (VPNs), VLAN segmentation and Access Control Lists (ACLs) to protect sensitive research data from cyber threats and unauthorized access. Cisco Packet Tracer was used to simulate and test the proposed network design. The system was evaluated through connectivity tests, packet inspection and simulated attack scenarios. The results showed that the implemented solution improved network confidentiality, integrity and availability by filtering malicious traffic, restricting unauthorized access and enabling secure remote communication.The study concludes that a firewall-centered secure network can significantly strengthen the cybersecurity posture of research institutions such as SIRDC while providing a scalable and cost-effective solution for protecting critical industrial and scientific data.

Table of Contents

APPROVAL FORM ..... **i**
Dedication ..... **ii**
Acknowledgement ..... **iii**
Abstract ..... **iii**
CHAPTER 1 ..... **7**
INTRODUCTION **7**
1.1 Introduction 7
1.2 Background of the Study 8
1.3 Statement of the Problem 8
1.4 Research Aim 9
1.5 Research Objectives 9
1.6 Research Questions 9
1.7 Significance of the Study 10
1.8 Assumptions 11
1.9 Limitations / Challenges 11
1.10 Scope / Delimitation of the Study 12
1.11 Definition of Terms 13
1.12 Summary 13
CHAPTER 2 ..... **14**
LITERATURE REVIEW **14**
2.1 Introduction 14
2.2 Theoretical Framework 14
2.3 The Evolution of Firewall Technology 15
2.4 Importance of Firewalls in Research Institutions 15
2.5 Common Cyber Threats in the Zimbabwean Context 16
2.6 Review of Related Empirical Studies 17
2.7 Identification of Research Gaps 17
2.8 Summary of Literature 18
CHAPTER 3 ..... **19**
RESEARCH METHODOLOGY **19**
3.1 Introduction 19
3.2 Types of Research 19
3.3 Research Design 20
3.4 Target Environment and Sampling 25

3.5 Sampling Technique and Sample Size 26
3.6 Data Collection Methods 27
3.7 Data Analysis Methods 28
3.8 Ethical Considerations 30
3.9 Reliability of the Study 31
3.10 Validity of the Study 31
3.11 Summary 31
CHAPTER 4 33
Data Presentation, Analysis and Interpretation 33
4.1 Introduction 33
4.2 Network Topology 33
4.3 IP Addressing Scheme 34
4.4 VLAN Segmentation Strategy 36
4.5 Inter-VLAN Routing 37
4.6 Firewall Policy Design 39
4.7 Intrusion Prevention System (IPS) 42
4.8 Virtual Private Network (VPN) Design 42
4.9 Quality of Service (QoS) 43
4.10 Network Security Policies 43
4.11 System Testing and Validation 44
4.12 Summary 44
CHAPTER 5 45
RESULTS, CONCLUSION AND RECOMMENDATIONS 45
5.1 Introduction 45
5.2 System Implementation Results 46
5.3 Network Connectivity Results 47
5.4 Firewall Performance Results 50
5.5 VLAN Segmentation Results 51
5.6 Intrusion Prevention System (IPS) Results 52
5.7 Conclusion 53
5.8 Recommendations 53
5.9 Summary 55
References 56
APPENDICES 57
Appendix A: Network Security Questionnaire 57

Appendix B: Key Informant Interview Guide 62
Appendix C: Signed Research Proposal 65

CHAPTER 1

INTRODUCTION

1.1 Introduction

In today's fast-paced world, data security and network integrity have emerged as critical pillars for organizational stability and national development. Modern industrial environments, characterized by the rapid digitization of intellectual property, sensitive research data and high-performance computing, face an escalating landscape of sophisticated cyber threats. The Scientific and Industrial Research and Development Center (SIRDC), as a hub for innovation and technological advancement, handles vast amounts of proprietary data that are essential to the nation's strategic growth. The increasing frequency of cyberattacks, unauthorized access and data breaches underscores the vulnerability of traditional networking frameworks.

Reports from global cybersecurity firms indicate that research institutions are prime targets for intellectual property theft, often leading to significant financial and reputational losses. These challenges highlight the need for a robust, Secure Network Infrastructure capable of providing real-time threat detection, data encryption and seamless connectivity across various research wings. The evolution of Firewalls, Virtual Private Networks (VPNs) and Intrusion Prevention Systems (IPS) has transformed the way organizations protect their digital assets. Intelligent network management tools and advanced cryptographic protocols can now continuously monitor traffic patterns, mitigate risks and ensure the confidentiality, integrity and availability of information. This study focuses on the Design and Implementation of a Secure Network for SIRDC, implementing firewalls to provide a resilient environment for scientific and industrial research.

1.2 Background of the Study

Network security and data integrity are closely interlinked processes that influence the operational stability and confidentiality of any research-driven organization. Persistent vulnerabilities in a network negatively impact data privacy, while frequent security breaches further degrade system trust and performance, creating a detrimental feedback loop of operational downtime and information loss. Traditional security methods, such as basic password protection and standalone antivirus software, are effective to a degree but are often reactive, insufficient against sophisticated modern threats and impractical for securing the complex data traffic of a multi-departmental institution.

Recent advances in Firewalls and software-defined security have provided opportunities for continuous, non-invasive network inspection through protocols that measure packet headers, traffic flow patterns and application-layer behavior. Integrating these technologies with features like Deep Packet Inspection (DPI), Intrusion Prevention Systems (IPS) and automated threat intelligence enhances the ability to identify anomalous patterns associated with cyber-attacks and unauthorized access. This evolution has paved the way for robust, intelligent and scalable defense mechanisms capable of protecting high-value intellectual property in real-time.

In Zimbabwe and other developing regions, the protection of scientific research and industrial data remains a significant challenge due to the high cost of proprietary security licenses and specialized infrastructure. A locally implemented and optimized firewall solution for the Scientific and Industrial Research and Development Center (SIRDC) can help the institution safeguard its technological innovations and enable administrators to manage the network perimeter effectively. This promotes a culture of digital resilience and ensures the secure advancement of national industrial research.

1.3 Statement of the Problem

The Scientific & Industrial Research and Development Center (SIRDC) currently lacks a centralized, high-performance firewall solution, leaving its network perimeter vulnerable to unauthorized external access and sophisticated cyber threats. Without a state-of-the-art firewall to monitor and filter incoming and outgoing traffic, SIRDC’s

critical research data and intellectual property are at high risk of exfiltration, threatening the integrity of its industrial development mission and operational continuity.

1.4 Research Aim

To design and implement a Secure Network Infrastructure for the Scientific and Industrial Research and Development Center (SIRDC), primarily focused on the deployment of a robust firewall to filter and secure data traffic patterns in real time.

1.5 Research Objectives

i. Develop and design strict security policies and firewall rules that regulate inbound and outbound traffic, ensuring only authorized communication occurs between network segments.

ii. Enforce Strict Access Controls by configuring granular firewall rules to prevent unauthorized traffic and data exfiltration.

iii. Provide Secure VPN Access to ensure authorized personnel can connect to research data remotely and safely

iv. Implement Intrusion Prevention (IPS) to automatically detect and block real-time cyber threats and malware.

1.6 Research Questions

i. What are the current vulnerabilities and threats present within the SIRDC network infrastructure?

ii. How can a multi-layered security architecture, incorporating elements such as firewalls, intrusion detection/prevention systems (IDS/IPS) and endpoint protection, be effectively designed and implemented to mitigate identified risks within the SIRDC network?

iii. How can continuous security monitoring and incident response capabilities be established and optimized within SIRDC to detect, analyze, and respond to cyber threats in real-

time?

iv. How can security awareness training programs be developed and delivered to SIRDC personnel to foster a strong security culture and minimize human-factor vulnerabilities within the network environment?

1.7 Significance of the Study

This study holds significant implications for the advancement of national cybersecurity infrastructure and the protection of industrial research assets. By integrating a robust Firewall into the SIRDC network, the project provides a platform for real-time monitoring of data traffic, allowing network administrators and security analysts to continuously track digital threats and unauthorized access attempts. Such continuous monitoring offers an opportunity for the early detection of network intrusions, ensuring timely intervention before security breaches escalate into serious data losses or system-wide failures.

Furthermore, the system promotes data-driven security management by providing administrators with accurate insights into daily traffic trends and potential attack vectors. These insights empower the institution to make informed infrastructure adjustments aimed at improving both the resilience and the performance of the research network. For the scientific community, this technology supports a secure collaborative environment, reducing the risk of intellectual property theft and enabling proactive rather than reactive threat management, particularly for sensitive industrial projects.

Lastly, the proposed solution emphasizes operational efficiency and resource optimization, making it a sustainable model for research institutions in developing economies. As highlighted in regional cybersecurity frameworks, developing cost-effective, scalable and high-performance network security solutions is crucial for improving technological sovereignty in resource-constrained environments such as Zimbabwe. The system therefore, contributes to the broader goal of promoting digital transformation and enhancing the security of national research through the application of smart, hardened network technologies.

1.8 Assumptions

The success of the proposed firewall implementation relies on several key assumptions that ensure the reliability and effectiveness of the network security framework. First, it is assumed that the network hardware and software interfaces integrated into the SIRDC infrastructure will accurately capture and log essential traffic parameters, such as packet headers, source/destination IPs and protocol behaviors. The precision of these logs is critical, as any missed packets or logging errors could compromise the integrity of the security audit and the accuracy of threat detection. It is further assumed that network traffic will consistently flow through the designated security gateway throughout the operational period, enabling continuous and reliable data inspection. Consistent routing is vital for establishing valid baseline traffic patterns and correlations between user behavior and potential security anomalies. Any bypass of the firewall or irregular routing configurations could result in security gaps or blind spots, thereby limiting the robustness of the threat analysis and the effectiveness of the filtering algorithms used in the system. Lastly, the study assumes that the firewall's hardware resources and processing engines will operate efficiently, with minimal latency and high throughput. This assumption ensures that real-time traffic filtering remains feasible without causing significant bottlenecks or disrupting the research activities of the institution. A reliable hardware and software environment will facilitate seamless packet inspection, secure encrypted tunnels (VPNs) and timely response to intrusions, which are essential for supporting accurate, real-time insights into the network's health status and for enabling prompt intervention by system administrators where necessary.

1.9 Limitations / Challenges

Despite its potential benefits, the proposed firewall-based network security system for SIRDC faces several anticipated challenges that could impact its overall performance and reliability. One of the primary limitations lies in the processing capacity and hardware specifications of the security appliance, which may affect the precision of deep packet inspection. Inconsistent hardware scaling or the use of legacy infrastructure could lead to bottlenecks in traffic analysis, ultimately compromising the speed and accuracy of threat detection outcomes.

Another significant challenge is the issue of upstream internet stability and power reliability, particularly within the local infrastructure context of Zimbabwe, where network outages or power fluctuations remain a factor. Limited or unstable connectivity may hinder real-time threat intelligence updates from cloud-based security databases, causing delays in identifying zero-day vulnerabilities. To mitigate this, the design may need to incorporate redundant power supplies (UPS) and local signature caching mechanisms to ensure that the internal network remains protected even during external disruptions.

Furthermore, encrypted traffic (SSL/TLS) poses another limitation to system visibility. As a significant portion of modern web traffic is encrypted, the firewall may face challenges in inspecting the contents of data packets without implementing intensive decryption protocols, which can consume high CPU resources. Additionally, high computational overhead presents a constraint on network performance, particularly during peak research hours. Significant latency could inconvenience SIRDC researchers and reduce productivity, underscoring the need for optimized filtering rules and high-performance hardware to maintain a secure environment without sacrificing network throughput.

1.10 Scope / Delimitation of the Study

The research focuses on designing and implementing a robust firewall-based security architecture for the SIRDC network to ensure non-invasive threat monitoring and data protection. The study will utilize security protocols to monitor parameters such as packet headers, traffic volume, source/destination IP addresses, port usage and application-layer behavior. Data will be routed through the firewall gateway and transmitted to a centralized management console via secure internal links for the analysis and visualization of network threats using Intrusion Prevention System (IPS) algorithms.

The study will primarily involve the SIRDC core local area network (LAN), focusing on protecting the research and development departments. While the system is designed to be scalable, the initial implementation will be delimited to the headquarters' network infrastructure, focusing on internal user traffic and external

gateway security to ensure that all researchers and administrative staff operate within a hardened digital environment.

1.11 Definition of Terms

i. **Firewall:** A network security system—either hardware or software-based—that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

ii. **Latency:** The time taken for a data packet to travel from sender to receiver, measured in milliseconds.

iii. **Network Integrity:** The state of a network where data is protected from unauthorized modification or deletion, ensuring that the information remains accurate and reliable.

iv. **VPN (Virtual Private Network):** A secure, encrypted tunnel between two or more devices, used to protect private network traffic from interception over public networks like the internet.

1.12 Summary

This chapter has introduced the background of the study, highlighting the critical importance of securing research data and underscoring the industrial imperative for a robust, preventative network defense system. It establishes the statement of the problem by detailing the inherent limitations of conventional, perimeter-based security and the deficiency of legacy networking equipment in providing the requisite multi-layered inspection (e.g., Deep Packet Inspection and Application-Layer Filtering) needed for accurate, real-time threat detection in dynamic, research-intensive settings.The chapter further outlined the research objectives aimed at creating a hardened digital environment for SIRDC and concludes by defining the study's scope and the significance of the study in contributing a validated, resilient and timely technological solution to the field of institutional network security and industrial data protection.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The purpose of this chapter is to provide a comprehensive review of existing literature, theories, and empirical studies related to network security and firewall implementation. In an era where data is considered an organization's most valuable asset, the mechanisms used to protect it must be robust, adaptive and intelligent. This review explores the fundamental concepts of network defense, the historical evolution of firewall technologies and the contemporary challenges faced by research-intensive organizations like the Scientific and Industrial Research and Development Center (SIRDC).

As noted by Moyo and Chikasha (2023) in the context of Zimbabwe's digital landscape, the transition toward digitized research environments has outpaced the implementation of adequate security frameworks. This disparity leaves institutions vulnerable to a myriad of cyber threats, ranging from data breaches to intellectual property theft. By synthesizing current research, this chapter establishes the theoretical foundation for the project, identifying gaps in traditional security measures and highlighting the necessity for firewalls.

2.2 Theoretical Framework

The cornerstone of network security is built upon the CIA Triad, a foundational model designed to guide security policies and protect organizational assets. For an institution like SIRDC, which manages high-value research data and industrial prototypes, the application of this triad through a robust firewall system is essential. Confidentiality ensures that sensitive research remains accessible only to authorized personnel; the firewall enforces this by utilizing Access Control Lists (ACLs) and encrypted Virtual Private Networks (VPNs) to shield internal communications from external eavesdropping. Integrity focuses on maintaining the accuracy and consistency of data throughout its lifecycle, with the firewall blocking malicious packets that attempt to

inject unauthorized code or modify research files during transit. Finally, Availability ensures that network resources remain accessible to legitimate users; by mitigating Distributed Denial of Service (DDoS) attacks and managing bandwidth, the firewall prevents the network from becoming overwhelmed by malicious traffic, ensuring that researchers can access critical data without interruption.

2.3 The Evolution of Firewall Technology

To understand the necessity of a secure network for SIRDC, it is vital to trace the historical progression of firewall technology from basic filters to the intelligent systems utilized in 2026. Early first-generation firewalls relied on simple packet filtering, which inspected data based on source and destination IP addresses but lacked the ability to detect malware hidden within the packets. This was followed by second-generation stateful inspection firewalls, which tracked the state of active connections but remained vulnerable to attacks targeting the application layer. Third-generation application-layer firewalls introduced the ability to filter traffic based on specific software or services, though often at the cost of high resource consumption and increased latency. Modern Next-Generation Firewalls (NGFW) represent a significant leap forward, combining Intrusion Prevention Systems (IPS) and Deep Packet Inspection (DPI) to provide comprehensive visibility. In the current landscape, AI-powered firewalls leverage machine learning to predict and neutralize zero-day threats, offering a proactive defense mechanism that is essential for institutions handling proprietary scientific data.

2.4 Importance of Firewalls in Research Institutions

Scientific and industrial research centers present unique security challenges because they require a delicate balance between open collaboration and rigorous data protection. Literature suggests that firewalls in these settings serve as critical "digital gatekeepers" that perform several specialized roles beyond simple traffic filtering. One primary function is network segmentation, which involves isolating sensitive research servers from general administrative traffic to limit the potential spread of a security breach. Additionally, firewalls provide active threat prevention by utilizing Intrusion Prevention Systems to block known exploit signatures in real-time before

they reach vulnerable local workstations. Finally, the integration of Data Loss Prevention (DLP) features allows the firewall to monitor outbound traffic, ensuring that proprietary Zimbabwean industrial innovations are not exfiltrated to unauthorized external servers. This multi-layered approach ensures that the institution can foster innovation within a hardened and resilient digital environment.

2.5 Common Cyber Threats in the Zimbabwean Context

The cybersecurity landscape in Zimbabwe has undergone a significant transformation, with reports indicating that by 2024, the country was ranked as the third most attacked nation globally. This heightened vulnerability is largely attributed to the rapid digital revolution and the "Fourth Industrial Revolution" (4IR), which have expanded the attack surface for local institutions. As highlighted by Maphosa (2023) and Manyaya (2024), organizations in Zimbabwe frequently face sophisticated threats such as email phishing, ransomware and identity theft. For a strategic research hub like SIRDC, these threats are not merely technical nuisances but direct risks to intellectual property and national scientific data. The high rate of counterfeit and pirated software in the region further exacerbates these risks, as such software often contains pre-installed malware that bypasses traditional, outdated security measures.

Furthermore, the Zimbabwean research and education sector has become a prime target for cybercriminals seeking high-value data and financial gain. Notable incidents, such as the ransomware attacks on major universities like the Harare Institute of Technology (HIT), where attackers demanded millions to restore encrypted data, underscore the critical deficiency in current network defenses. These attacks often leverage social engineering and zero-day exploits to infiltrate networks that lack a comprehensive security culture or modern technical safeguards. Consequently, the absence of a robust national cybersecurity implementation plan makes it imperative for institutions to adopt self-contained, highperformance security infrastructures such as the firewall system proposed in this study to protect their digital assets from an increasingly hostile environment.

2.6 Review of Related Empirical Studies

Empirical studies conducted within Zimbabwe and the broader SADC region highlight a recurring theme of inadequate technical controls and a lack of formalized security frameworks. A study by Mashizha and Kanengoni (2025) on the adequacy of cybersecurity in local institutions found that most security mechanisms are "a step behind" the methods currently used by cybercriminals, with many organizations still lacking a basic cybersecurity framework. This research revealed that while network and data security are ranked as top priorities for technical experts, the implementation of these measures is often hindered by limited skills, obsolete IT infrastructure and a lack of executive financial support. This "afterthought" approach to security, as noted by Kabanda (2019), is worsened by a brain drain of skilled personnel, leaving vital infrastructure like SIRDC's network exposed to persistent threats.

Internationally, the effectiveness of firewalls in mitigating these risks has been widely documented. Research suggests that integrating Deep Packet Inspection (DPI) and Intrusion Prevention Systems (IPS) can reduce successful malware infiltrations by over 70% compared to traditional packet filters. Locally, however, there is a significant gap in documented implementations of these advanced systems within industrial research centers. Current literature primarily focuses on the financial sector, leaving a research void regarding the specific network security requirements of scientific organizations. This project seeks to address this gap by documenting the practical implementation of a firewall-centered architecture, providing an empirical reference for other Zimbabwean research and development institutions.

2.7 Identification of Research Gaps

The primary gap identified in this review is the lack of documented, localized technical implementations of high-performance firewall architectures within scientific and industrial research centers like SIRDC. While there is a wealth of information on cybersecurity governance and the "human factor," there is a deficiency in empirical data regarding the configuration and performance of hardware-based security in protecting proprietary Zimbabwean research data. Furthermore, although the Zimbabwe Cyber and Data Protection Act (2021) provides a legal framework, many

institutions still lack a technical blueprint for transitioning from traditional packet filtering to comprehensive application-layer defense. This study seeks to bridge this gap by providing a practical framework for implementing a secure network, thereby establishing a technical reference for other research and development organizations in resource-constrained environments.

2.8 Summary of Literature

The literature review has demonstrated that network security has evolved from simple packet filtering to complex, AI-driven Next-Generation Firewalls (NGFW) capable of deep packet inspection. Research indicates that the shift toward the Fourth Industrial Revolution (4IR) and increased internet penetration has significantly expanded the attack surface for local institutions, yet defensive frameworks in developing nations remain largely reactive. Current studies emphasize that organizations are increasingly vulnerable to ransomware, phishing, and zero-day exploits, particularly in environments where legacy hardware is prevalent. While international literature underscores the efficacy of advanced firewalls in mitigating these risks, the regional discourse in Zimbabwe remains heavily focused on the financial sector and high-level policy awareness, rather than technical implementation in researchintensive environments.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

In this chapter, the researcher details the research methodology adopted for the design, configuration and implementation of the firewall system at the Scientific and Industrial Research and Development Center (SIRDC). This project aims to enhance the institution's cybersecurity posture by providing a robust defense mechanism against the evolving threat landscape identified in the previous chapter. By employing a systematic technical approach, the study seeks to analyze current network vulnerabilities, implement an intelligent trafficfiltering architecture, and validate the system's effectiveness in securing sensitive Zimbabwean research and industrial data. The following sections will outline the research design, the target network environment, data collection methods, technical instrumentation, and the evaluation techniques involved in this implementation.

3.2 Types of Research

To ensure a comprehensive approach to the security challenges at SIRDC, this study employs three specific types of research:

3.2.1 Applied Research

This project is categorized as Applied Research because it is designed to solve a specific, practical problem facing a real-world institution. Rather than seeking to develop new general theories about cybersecurity, the focus is on applying existing firewall technologies and security protocols to harden the SIRDC network against documented threats. The primary goal is to produce a functional solution that has immediate utility for the organization.

3.2.2 Quantitative Research

The evaluation phase of the firewall implementation relies on a Quantitative approach. This involves the collection and analysis of numerical data to measure the system's effectiveness. Key metrics include:

Throughput and Latency: Measuring network speed before and after firewall installation.

Packet Loss: Quantifying the amount of data dropped during high-traffic periods.

Threat Detection Rates: Counting the number of blocked intrusion attempts or malicious packets during the testing phase.

3.2.3 Explanatory Research

The study also utilizes Explanatory Research to establish cause-and-effect relationships within the network environment. This type of research helps to explain why certain vulnerabilities exist in the current SIRDC infrastructure and how the specific configuration of the firewall (such as Deep Packet Inspection) directly mitigates those specific risks.

3.3 Research Design

The researcher adopted a Design Science Research (DSR) design for this study. This design is specifically chosen because it focuses on the development and evaluation of technical "artifacts"—in this case, the firewall system—to solve a specific organizational problem at SIRDC. Unlike traditional descriptive research that merely observes a situation, DSR is proactive and involves a cyclical process of designing, implementing, and testing a solution.

3.3.1 System Design Tools Used

The implementation and simulation of the proposed secure network infrastructure for SIRDC utilized several system design and network security tools to support network modeling, configuration and testing. These tools enabled the researcher to develop, simulate and validate the firewall-based architecture within a controlled virtual environment.

I. Cisco Packet Tracer

Cisco Packet Tracer was used as the primary network simulation tool for designing and testing the secure network infrastructure. The software enabled the configuration of routers, switches, VLANs, firewalls, Access Control Lists (ACLs), VPNs and routing protocols within a virtualized environment. It also

provided simulation mode functionality for analyzing packet flow, connectivity and firewall filtering behavior.

Fig 3.3.1 Cisco Packet Tracer



II. Routers

Routers were used to connect different network segments and provide communication between the internal SIRDC network and external internet services. The router also handled routing functions, traffic forwarding and policy-based routing within the network infrastructure.

Fig 3.3.2 Router



III. Layer 3 Core Switch

The Layer 3 Core Switch was used to perform inter-VLAN routing and high-speed data forwarding between different departments within the SIRDC network. It also acted as the central backbone of the network architecture.

Fig 3.3.3 Core switch(3 layer switch)



IV. Access Switches

Access switches were used to connect end-user devices such as workstations, servers and administrative computers to their respective VLANs. These switches helped enforce network segmentation and improve traffic management.

Fig 3.3.4 Access switch(Layer2 switch)



V. Servers

Servers were deployed within the DMZ and internal network to provide services such as web hosting, file sharing, email filtering and research database management. These servers supported both internal operations and secure external access.



Fig 3.3.5 servers

VI. Cisco ASA Firewall

The Cisco Adaptive Security Appliance (ASA) firewall was used to implement network perimeter security. The ASA firewall provided functionalities such as packet filtering, Network Address Translation (NAT), Intrusion Prevention System (IPS) integration and Virtual Private Network (VPN) services. It was configured to enforce strict security policies between the internal network, DMZ and external internet connections.

Fig 3.3.6 Cisco ASA Firewall



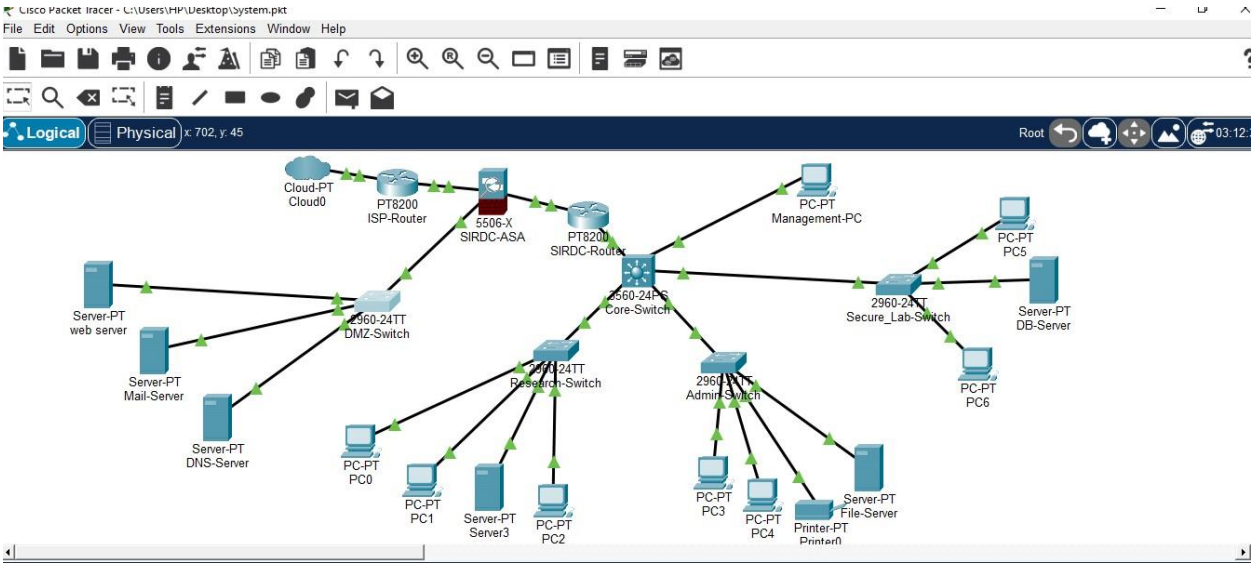
VII. End-User Workstations

Workstations represented the computers used by researchers, administrators and network managers within the SIRDC environment. These devices were used during connectivity testing, traffic simulations and access control validation. *Fig 3.3.7 End users*



Full network topology

Fig 3.3.1 Network design



The design follows a structured five-step process:

i. **Requirement Analysis:** Identifying the specific security needs and "pain points" within the SIRDC network.

ii. **System Design:** Drafting the logical and physical architecture of the firewall, including the rulesets and DMZ (Demilitarized Zone) configurations.

iii. **Implementation:** The actual deployment and configuration of the firewall hardware or software within the live network environment.

iv. **Testing and Evaluation:** Subjecting the system to simulated network stresses and security threats to measure its performance.

v. **Documentation:** Reporting the findings and final configuration settings to serve as a technical blueprint for the institution.

3.4 Target Environment and Sampling

The target environment for this research is the Local Area Network (LAN) of the Scientific and Industrial Research and Development Center (SIRDC), specifically focusing on the gateway interface and the high-security segments that house proprietary research databases and industrial prototypes. To effectively analyze and secure this environment, the study employs purposive sampling to isolate critical

network traffic segments rather than monitoring the entire, undifferentiated data flow. This sampling technique ensures that the research focuses on "High-Value Targets" (HVT), such as traffic directed toward sensitive servers and administrative nodes, allowing for a more focused evaluation of the firewall's ability to protect the institution's most vital intellectual property and digital assets.

3.5 Sampling Technique and Sample Size

This study utilizes a purposive sampling technique, a non-probability sampling method where the researcher deliberately selects specific network segments and data points based on their strategic importance to the organization. For an institution like the Scientific and Industrial Research and Development Center (SIRDC), which manages high-value proprietary data, this technique is more effective than random sampling as it allows the researcher to focus on "critical case sampling." By specifically targeting the gateway interfaces, research-intensive servers and administrative databases, the researcher ensures that the firewall's security policies are tested against the most vital and vulnerable areas of the network. This judgment-based approach is essential for identifying the specific traffic patterns and potential attack vectors that pose the greatest risk to SIRDC's intellectual property.

The sample size for this technical implementation is determined by the specific network nodes and traffic volume required to provide a statistically significant evaluation of the firewall's performance. The researcher has selected a sample of ten critical network devices, comprising the primary external gateway, two central research servers and five workstations within the industrial development department. To validate the system's efficiency under varying loads, a sample of network traffic logs will be collected and analyzed over a continuous 72-hour window. This sampling period is designed to capture a representative mix of peak operational traffic and off-peak idle periods, totaling approximately 3000 connection sessions, which provides a robust dataset for measuring throughput, latency and the accuracy of the firewall's threat-detection mechanisms.

3.6 Data Collection Methods

Since this project is implemented within a virtualized environment, data collection is conducted through Simulated Network Observation and Experimental Prototyping. The researcher uses the built-in diagnostic features of Cisco Packet Tracer to gather quantitative data on how the firewall processes traffic.

3.6.1 Simulation-Based Data Capture

The primary source of data is the Cisco Packet Tracer Simulation Mode. This allows the researcher to capture "Time-Frozen" snapshots of the network. Data collection includes:

PDU (Protocol Data Unit) Inspection: Capturing individual packets (ICMP, TCP, HTTP) as they arrive at the firewall interface to verify if they are permitted or denied based on the configured Access Control Lists (ACLs).

ICMP Echo Requests (Ping): Using the "Ping" command to collect success/failure rates, which provides binary data (Success/Fail) on the connectivity and security of specific network paths.

Packet Tracer CLI Output: Utilizing the Command Line Interface (CLI) to run show commands (e.g., show access-lists or show ip nat translations). These outputs provide the raw data required to verify that the firewall is correctly identifying and counting "hits" on specific security rules.

3.6.2 Comparative Performance Data

To evaluate the effectiveness of the implementation, data is collected in two distinct simulation stages:

Pre-Implementation Baseline: Running connectivity tests on a simulated SIRDC network without a firewall to identify existing security gaps and open access points.

Post-Implementation Validation: Repeating the same tests after the firewall/ASA (Adaptive Security Appliance) is configured. The delta (difference) between these two datasets provides the quantitative evidence of the firewall's impact on network security.

3.6.3 Scenario-Based Threat Simulation

The researcher gathers data by purposefully initiating "unauthorized" traffic from a simulated external "Attacker PC" within Packet Tracer. Data is collected on whether the firewall successfully drops these packets and logs the unauthorized attempt, providing empirical proof of the system's defensive capabilities.

3.7 Data Analysis Methods

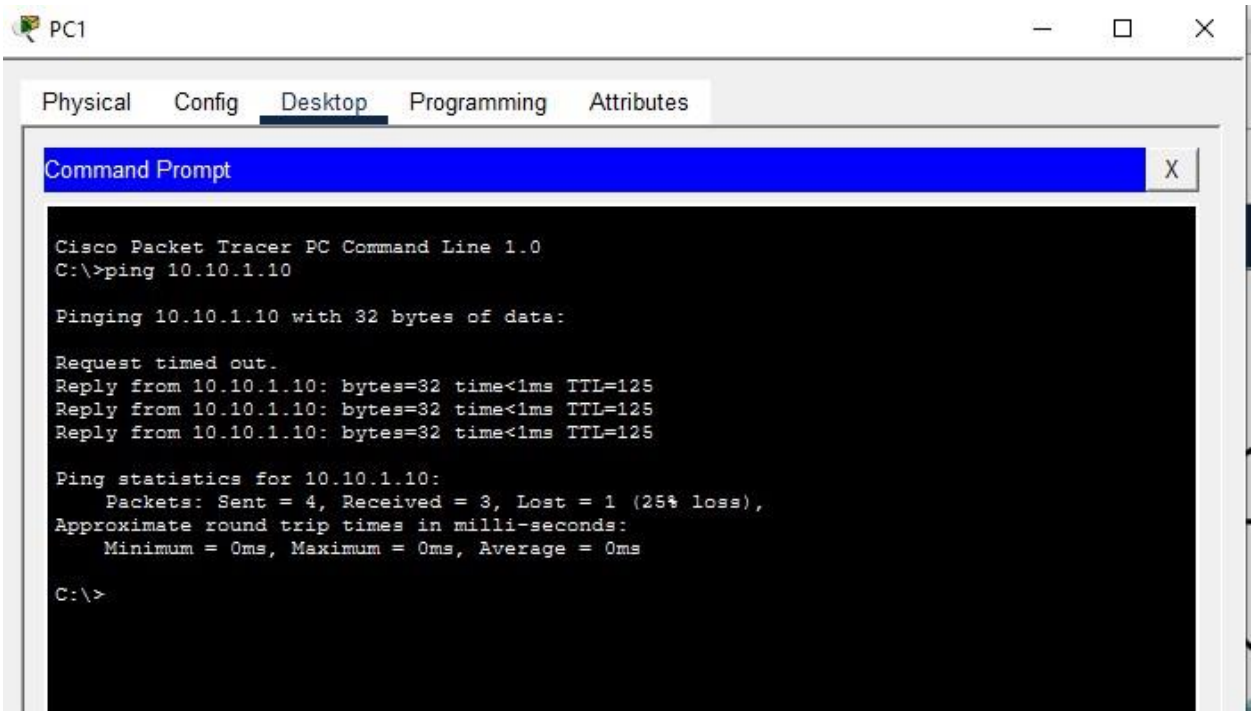
The data analysis for this project is conducted through a structured comparison of the network's behavior before and after the firewall implementation within the Cisco Packet Tracer environment. The researcher employs both quantitative and qualitative analysis techniques to interpret the results generated by the simulation.

3.7.1 Quantitative Analysis

Quantitative data is analyzed by measuring specific network performance metrics and security outcomes. This involves:

Connectivity and Blocking Rates: The researcher uses the success/failure results of ICMP (Ping) tests and HTTP requests to calculate the percentage of unauthorized traffic successfully blocked by the firewall versus legitimate traffic allowed.

Fig 3.7.1 Ping test



Access Control List (ACL) Hit Counts: By utilizing the show access-lists command in the CLI, the researcher analyzes the "hit count" for each rule. This provides numerical evidence of how many times specific security policies were triggered by simulated traffic.

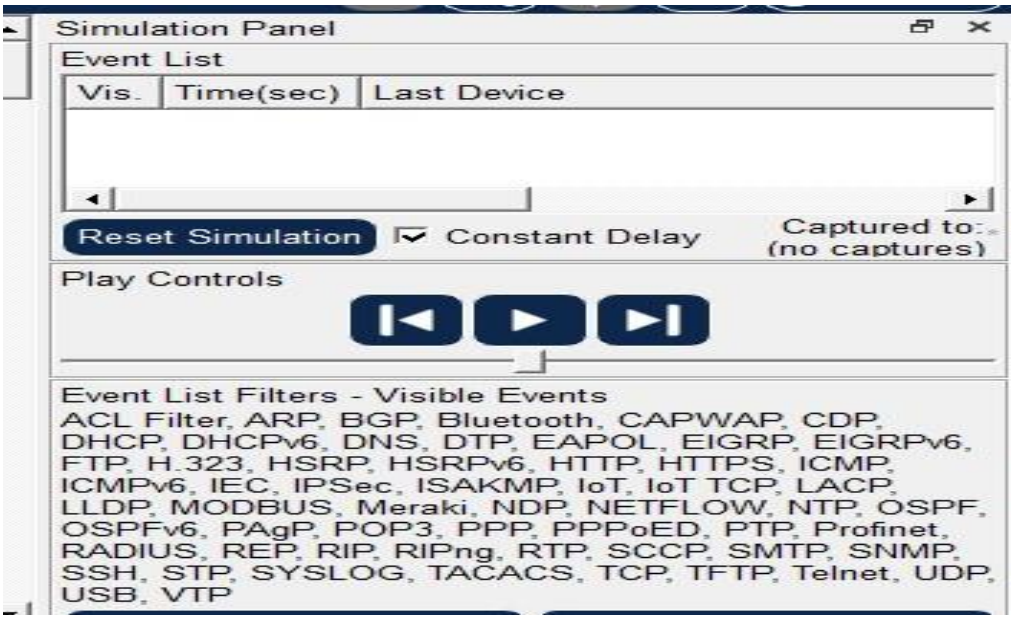
Throughput and Latency Metrics: The researcher analyzes the time taken for packets to traverse the network in "Simulation Mode," comparing the delay introduced by the firewall's inspection process against the baseline network speed.

3.7.2 Qualitative Analysis

Qualitative analysis focuses on the logical flow and integrity of the security architecture. This includes:

Packet Flow Visualization: Using the Simulation Mode Event List, the researcher performs a step-by-step visual analysis of packet paths. This qualitative check ensures that packets are being dropped at the correct interface (e.g., the outside interface of the ASA) rather than leaking into the internal network.

Fig 3.7.2 : Simulation Mode



OSI Layer Inspection: The researcher analyzes the "Inbound PDU Details" and "Outbound PDU Details" for filtered packets. This helps in understanding at which layer of the OSI model the firewall is making its decision (e.g., Layer 3 for IP filtering or Layer 4 for Port blocking), ensuring the implementation aligns with the theoretical framework of the CIA Triad.

Security Policy Validation: The researcher reviews the configuration logic to ensure that the "Principle of Least Privilege" is maintained, qualitatively assessing if the ruleset is too permissive or if it correctly isolates SIRDC's high-value research assets.

3.8 Ethical Considerations

In conducting this study, the researcher adheres to the ethical standards governing information technology research and institutional security. Since the project involves designing a security framework for a strategic national institution like the Scientific and Industrial Research and Development Center (SIRDC), confidentiality is paramount; all simulated network configurations and IP addressing schemes are treated as sensitive data to prevent providing a potential blueprint for real-world exploits. The use of Cisco Packet Tracer further ensures the principle of non-

maleficence, as it allows for rigorous testing of restrictive security policies and simulated attacks without causing actual downtime or disruption to SIRDC's live production environment. Furthermore, the researcher maintains academic integrity by reporting all simulation outcomes truthfully, including any configuration limitations, while ensuring that the proposed monitoring and logging features comply with the privacy requirements outlined in the Zimbabwe Cyber and Data Protection Act of 2021.

3.9 Reliability of the Study

Reliability refers to the consistency of research procedures and results (Saunders et al., 2019). In this study, reliability was ensured through the use of standardized firewall configurations, repeated simulation tests and controlled network environments within Cisco Packet Tracer. Tests such as ping requests, ACL verification and unauthorized access simulations were repeated under the same conditions to ensure consistent results. The use of command-line verification tools also helped maintain stable and accurate configurations throughout the study.

3.10 Validity of the Study

Validity refers to the extent to which a study accurately measures what it intends to measure (Creswell & Creswell, 2018). The validity of this study was ensured by aligning the firewall implementation with the identified cybersecurity challenges at SIRDC. The research incorporated recognized security principles such as the CIA Triad, defense-in-depth and least privilege access control (Stallings, 2018). Furthermore, realistic network simulations and measurable security indicators such as intrusion blocking rates, ACL hit counts and latency measurements were used to evaluate the effectiveness of the proposed secure network infrastructure.

3.11 Summary

This chapter has established a comprehensive methodological framework for the design and evaluation of the firewall system at SIRDC. By adopting a Design Science Research paradigm, the study transitions from theoretical security concepts to a

practical, simulationbased implementation using Cisco Packet Tracer. The use of purposive sampling ensures that the most critical network nodes and traffic segments are prioritized, while the data collection and analysis methods provide a structured way to measure success through both quantitative hit-counts and qualitative packet-flow inspections. Finally, the ethical framework guarantees that the research is conducted safely within a virtual environment, respecting both institutional confidentiality and national data protection regulations. This methodology provides a rigorous foundation for the subsequent system design and implementation phases detailed in the following chapter.

CHAPTER 4

Data Presentation, Analysis and Interpretation

4.1 Introduction

This chapter presents the implementation, analysis and interpretation of the proposed secure network infrastructure for the Scientific and Industrial Research and Development Center (SIRDC). The chapter focuses on the configuration and evaluation of the firewall-based security architecture designed using Cisco Packet Tracer. The implementation incorporates VLAN segmentation, inter-VLAN routing, firewall security policies, Intrusion Prevention Systems (IPS), Virtual Private Networks (VPNs) and Quality of Service (QoS) mechanisms to enhance the confidentiality, integrity and availability of institutional data.

The chapter further presents the network topology, IP addressing scheme, firewall configurations and simulation results obtained during system testing. The effectiveness of the proposed network design is evaluated through connectivity tests, access control verification and simulated cyberattack scenarios to determine the ability of the system to secure sensitive research and industrial information at SIRDC.

4.2 Network Topology

The proposed network topology adopts a five-layer hierarchical design consisting of:

1. Edge Layer: ISP Router providing Internet connectivity
2. Security Layer: Firewall performing IPS, VPN, and Deep Packet Inspection
3. Distribution Layer: SIRDC Router handling WAN aggregation, QoS, and policybased routing
4. Core Layer: Layer 3 Core Switch providing high-speed inter-VLAN routing
5. Access Layer: VLAN-specific switches connecting end-user devices

Figure 4.1 illustrates the complete network topology for SIRDC:

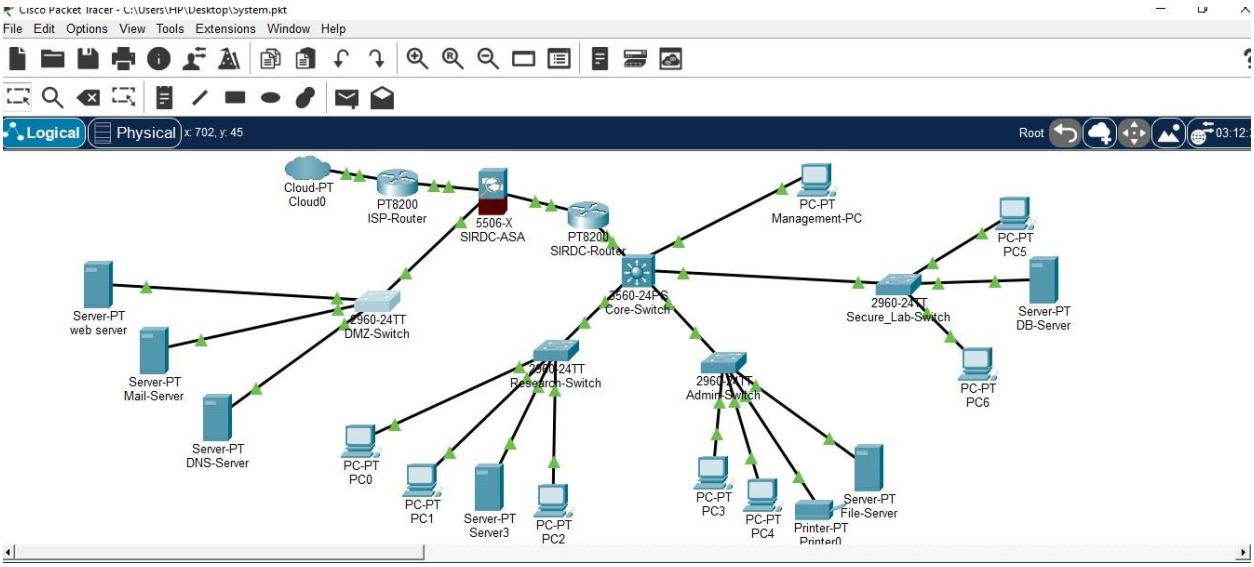


Figure 4.1: SIRDC Secure Network Topology

4.3 IP Addressing Scheme

Table 4.1 presents the complete IP addressing scheme for all network devices and subnets.

Device / Network	Interface / Subnet	IP Address	Purpose
ISP Router	WAN (Internet)	DHCP / Static Public	Internet uplink
ISP Router	LAN to Firewall	203.0.113.1/30	Upstream gateway
SIRDC Firewall	Outside (WAN)	203.0.113.2/30	ISP connection
SIRDC Firewall	Inside (LAN)	192.168.0.1/30	Transit to SIRDC Router
SIRDC Firewall	Management	10.10.10.1/24	Admin access only
SIRDC Router	WAN (to Firewall)	192.168.0.2/30	Default gateway from firewall
SIRDC Router	LAN (to Core Switch)	192.168.1.1/29	Transit to Core Switch
SIRDC Router	Loopback	10.255.255.1/32	Router OOB management
SIRDC Core Switch	SVI to Router (VLAN 1)	192.168.1.2/29	Uplink to router

SIRDC Core Switch	VLAN 10 SVI	10.10.1.1/24	Gateway for DMZ
SIRDC Core Switch	VLAN 20 SVI	10.20.0.1/24	Gateway for Research
SIRDC Core Switch	VLAN 30 SVI	10.30.0.1/24	Gateway for Admin
SIRDC Core Switch	VLAN 40 SVI	10.40.0.1/24	Gateway for Secure Lab
SIRDC Core Switch	VLAN 99 SVI	10.10.10.2/24	Device management
DMZ Switch	Access ports (VLAN 10)	N/A	DMZ device connectivity
Research Switch	Access ports (VLAN 20)	N/A	R&D device connectivity
Admin Switch	Access ports (VLAN 30)	N/A	Admin device connectivity
Secure Lab Switch	Access ports (VLAN 40)	N/A	Secure lab device connectivity
Web Server	DMZ VLAN 10	10.10.1.10/24	Public web services
Mail Relay	DMZ VLAN 10	10.10.1.20/24	Email filtering
R&D Workstation	Research VLAN 20	DHCP (10.20.0.100200)	Research staff
HPC Cluster	Research VLAN 20	10.20.1.10/24	High-performance computing
Admin PC	Admin VLAN 30	DHCP (10.30.0.100200)	Staff workstations
File Server	Admin VLAN 30	10.30.0.250/24	Internal file sharing
Research Database	Secure Lab VLAN 40	10.40.0.10/24	Proprietary research data
Prototype Systems	Secure Lab VLAN 40	10.40.0.20/24	Industrial prototypes
Management PC	Management VLAN 99	10.10.10.10/24	Network device console
VPN Pool	Remote Access	172.16.10.0/24	VPN client assignments

Table 4.1: SIRDC IP Addressing Scheme

4.4 VLAN Segmentation Strategy

To enhance security, scalability and traffic management within the SIRDC network, a Virtual Local Area Network (VLAN) segmentation strategy is implemented. VLANs logically divide the network into smaller broadcast domains, reducing congestion and isolating sensitive resources.

The proposed VLAN structure is as follows:

VLAN 10 – DMZ Network

Hosts publicly accessible servers such as the web server and mail relay. This zone is exposed to external traffic but strictly controlled by firewall rules.

VLAN 20 – Research Network

Dedicated to research staff and high-performance computing systems. This VLAN handles sensitive experimental data and requires high bandwidth and strict access control.

VLAN 30 – Administrative Network

Used by administrative staff for routine operations such as documentation and internal communication.

VLAN 40 – Secure Lab Network

Contains highly confidential research databases and prototype systems. This VLAN is heavily restricted and accessible only to authorized personnel.

VLAN 99 – Management Network

Reserved for network administrators to manage infrastructure devices such as routers, switches, and firewalls.

Fig 4.3 : showing created Vlans

```
SIRDC-CoreSW>en
SIRDC-CoreSW#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/2
10   DMZ                              active
20   Research                         active
30   Admin                            active
40   SecureLab                        active
99   Management                       active    Fa0/5
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SIRDC-CoreSW#
```

This segmentation enforces the principle of least privilege, ensuring that users only access resources necessary for their roles.

4.5 Inter-VLAN Routing

Inter-VLAN communication is managed by the Layer 3 Core Switch, which facilitates traffic between segments via Switched Virtual Interfaces (SVIs). Each VLAN is assigned a specific gateway IP address on the switch to serve as its default exit point:

VLAN	**Segment Name**	**Gateway IP Address**
VLAN 10	DMZ	10.10.1.1
VLAN 20	Research	10.20.0.1
VLAN 30	Admin	10.30.0.1
VLAN 40	Secure Lab	10.40.0.1
VLAN 99	Management	10.10.10.2

Figure 4.5.1: SIRDC Inter-VLAN

```
SIRDC-CoreSW>
SIRDC-CoreSW>en
SIRDC-CoreSW#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  up                    up
FastEthernet0/3        unassigned      YES unset  up                    up
FastEthernet0/4        unassigned      YES unset  up                    up
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  down                  down
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     192.168.1.2     YES manual up                    up
GigabitEthernet0/2     unassigned      YES unset  down                  down
Vlan1                  unassigned      YES unset  administratively down down
Vlan10                 10.10.1.1       YES manual up                    down
Vlan20                 10.20.0.1       YES manual up                    up
Vlan30                 10.30.0.1       YES manual up                    up
Vlan40                 10.40.0.1       YES manual up                    up
Vlan99                 10.10.10.2      YES manual up                    up
SIRDC-CoreSW#
SIRDC-CoreSW#
```

Routing Policies and Access Control

To bolster internal security and prevent unauthorized lateral movement, specific routing policies are enforced:

1) **Selective Access:** The Research VLAN (20) is permitted to communicate with DMZ servers for data processing.
2) **Segment Isolation:** The Admin VLAN (30) is strictly prohibited from accessing the Secure Lab (40).
3) **Hardened Environment:** The Secure Lab VLAN (40) remains fully isolated, granting entry only to verified, authorized traffic.

By centralizing control at the Core Switch, the network minimizes the attack surface and ensures that internal data flows strictly follow the principle of least privilege.

Figure 4.5.2: ***Routing Policies and Access Control***

```
SIRDC-CoreSW>en
SIRDC-CoreSW#show ip access-lists
Extended IP access list BLOCK_ADMIN_TO_SECLAB
    10 deny ip 10.30.0.0 0.0.0.255 10.40.0.0 0.0.0.255
    20 permit ip any any
Extended IP access list RESEARCH_TO_DMZ
    10 permit ip 10.20.0.0 0.0.0.255 10.10.1.0 0.0.0.255
    20 deny ip 10.20.0.0 0.0.0.255 10.40.0.0 0.0.0.255
    30 permit ip any any
Extended IP access list ADMIN_POLICY
    10 deny ip 10.30.0.0 0.0.0.255 10.40.0.0 0.0.0.255 (12 match(es))
    20 deny ip 10.30.0.0 0.0.0.255 10.20.0.0 0.0.0.255
    30 permit ip any any (2 match(es))
Extended IP access list RESEARCH_POLICY
    10 deny ip 10.20.0.0 0.0.0.255 10.40.0.0 0.0.0.255 (4 match(es))
    20 permit ip 10.20.0.0 0.0.0.255 10.10.1.0 0.0.0.255 (25 match(es))
    30 permit ip any any (61 match(es))

SIRDC-CoreSW#
```

4.6 Firewall Policy Design

The firewall serves as the primary security gateway, enforcing granular traffic filtering and stateful inspection between disparate network segments.

4.6.1 Firewall Zones

The architecture is divided into three distinct logical zones to isolate assets based on risk:

i. Outside Zone (Untrusted): The public internet. ii. Inside Zone (Trusted): The private internal LAN.

iii. DMZ Zone (Semi-Trusted): An isolated segment for public-facing services (e.g., web and mail servers).

Figure 4.6.1 Firewall zones

```
hostname SIRDC-Firewall
names
!
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 203.0.113.2 255.255.255.252
!
interface GigabitEthernet1/2
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.252
!
interface GigabitEthernet1/3
 nameif dmz
 security-level 50
 ip address 10.10.1.1 255.255.255.0
!
```

4.6.2 Access Control Policies

Access Control Lists (ACLs) enforce the "Principle of Least Privilege" across all zones:

Direction	**Permitted Traffic**	**Protocol/Port**	**Action**
Internet → DMZ	Web & Mail Services	HTTP (80), HTTPS (443), SMTP (25)	Allow
Internet → LAN	All Traffic	N/A	Explicit Deny
LAN → Internet	Web & Core Services	HTTP/HTTPS ,DNS	Allow
All Other	Unidentified Traffic	Any	Implicit Deny

Fig 4.6.2 Access control list

```
!
access-list OUTSIDE_IN extended permit tcp any host 10.10.1.10 eq www
access-list OUTSIDE_IN extended permit tcp any host 10.10.1.10 eq 443
access-list OUTSIDE_IN extended permit tcp any host 10.10.1.20 eq smtp
access-list OUTSIDE_IN extended deny ip any any
access-list OUTSIDE_IN extended permit icmp any any
access-list DMZ_IN extended permit tcp host 10.10.1.10 10.0.0.0 255.0.0.0
access-list DMZ_IN extended permit icmp host 10.10.1.10 10.0.0.0 255.0.0.0
access-list INSIDE_OUT extended permit ip 10.0.0.0 255.0.0.0 any
access-list INSIDE_OUT extended permit ip 192.168.0.0 255.255.255.0 any
access-list INSIDE_OUT extended permit ip 192.168.1.0 255.255.255.248 any
access-list INSIDE_OUT extended deny ip any any
!
!
access-group OUTSIDE_IN in interface outside
access-group DMZ_IN in interface dmz
!
```

4.6.3 Network Address Translation (NAT)

NAT is utilized to mask internal topology and optimize address space:

Static NAT: Provides a one-to-one mapping between public IP addresses and specific DMZ servers.

Dynamic NAT/PAT: Maps multiple internal hosts to a single public IP, allowing safe outbound internet access for the LAN.

Fig 4.6.3 Network Address Translation

```
!
object network ALL_INTERNAL
 subnet 10.0.0.0 255.0.0.0
 nat (inside,outside) dynamic interface
object network LAN_INSIDE
 subnet 192.168.0.0 255.255.255.0
 nat (inside,outside) dynamic interface
object network MAIL_RELAY
 host 10.10.1.20
 nat (dmz,outside) static 203.0.113.11
object network MAIL_SERVER
 host 10.10.1.20
 nat (dmz,outside) static 203.0.113.11
object network WEB_SERVER
 host 10.10.1.10
 nat (dmz,outside) static 203.0.113.10
!
```

4.7 Intrusion Prevention System (IPS)

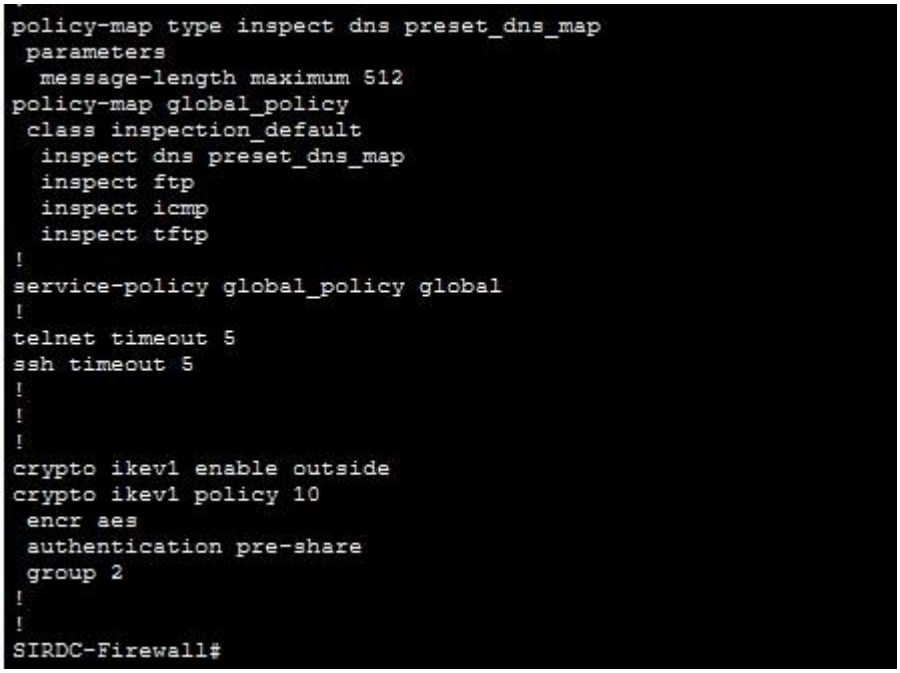
Integrated directly into the firewall, the IPS provides real-time threat mitigation through:

Signature-Based Detection: Identifying known exploit patterns and malware.

Anomaly-Based Analysis: Flagging deviations from baseline network behavior.

Active Response: Automatically dropping packets from suspicious IP addresses to prevent DoS attacks and port scanning.

Fig 4.7 Intrusion Prevention System



4.8 Virtual Private Network (VPN) Design

To support a secure mobile workforce, an IPsec VPN provides an encrypted "tunnel" for remote access.

Authentication: Multi-factor credentials ensure only verified users connect.

Client Pool: Remote users are assigned IPs from the 172.16.10.0/24 range.

Access Scope: Encrypted paths are restricted to essential research databases and internal management systems.

4.9 Quality of Service (QoS)

QoS policies prioritize bandwidth-heavy and mission-critical traffic to ensure stability:

High Priority: Research data transfers and High-Performance Computing (HPC) traffic.

Medium Priority: General administrative and operational traffic.

Low Priority: Non-critical web browsing and social

media. *Fig 4.9: Quality of sercives (QOS)*

```
policy-map SIRDC_QOS
 class HIGH_PRIORITY
  priority percent 30
 class MEDIUM_PRIORITY
  bandwidth percent 20
 class LOW_PRIORITY
  bandwidth percent 10
!
!
!
!
!
interface Loopback0
 ip address 10.255.255.1 255.255.255.255
!
interface GigabitEthernet0/0/0
 description "WAN - to Firewall Inside"
 ip address 192.168.0.2 255.255.255.252
 service-policy output SIRDC_QOS
 duplex auto
 speed auto
!
```

4.10 Network Security Policies

Beyond technical controls, the network is governed by administrative security standards:

Identity Management: Enforced strong password complexity and Role-Based Access Control (RBAC).

Maintenance: Mandatory periodic system patching and firmware updates.

Auditability: Centralized logging and continuous monitoring for incident response.

4.11 System Testing and Validation

The integrity of the design was verified using Cisco Packet Tracer, simulating real-world traffic scenarios.

Connectivity: Validated successful Ping and HTTP requests between authorized nodes. *Fig 4.11.1 unauthorized node*

```
C:\>nslookup www.sirdc.ac.zw

Server: [10.10.1.30]
Address:  10.10.1.30

Non-authoritative answer:
Name:   www.sirdc.ac.zw
Address:   10.10.1.10
```

Security Audits: Tested firewall efficacy by attempting unauthorized cross-VLAN access.

Fig 4.11.1 unauthorized cross VLAN access

```
C:\>
C:\>ping 10.40.0.100

Pinging 10.40.0.100 with 32 bytes of data:

Reply from 10.20.0.1: Destination host unreachable.
Reply from 10.20.0.1: Destination host unreachable.
Reply from 10.20.0.1: Destination host unreachable.
Reply from 10.20.0.1: Destination host unreachable.

Ping statistics for 10.40.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Performance Metrics: Ensured firewall processing introduced negligible latency to critical data flows.

4.12 Summary

This chapter provided an in-depth analysis of the SIRDC secure network architecture, detailing a multi-layered defense strategy. By centralizing inter-VLAN routing on a Layer 3 Core Switch and implementing strict SVI-based gateways, the design ensures logical isolation of sensitive departments. The integration of stateful firewalling and Intrusion Prevention Systems (IPS) establishes a robust perimeter, while IPsec VPN

protocols extend this security to remote access. Together with QoS traffic prioritization and Role-Based Access Controls, these components form a resilient, scalable infrastructure designed to mitigate lateral movement and defend against evolving cyber threats.

CHAPTER 5

RESULTS, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the results obtained from the implementation and testing of the proposed Secure Network Infrastructure for the Scientific and Industrial Research and Development Center (SIRDC). The chapter evaluates the effectiveness of the firewallcentered security architecture in protecting sensitive research data, controlling unauthorized access and improving the overall security posture of the institution. The findings are based on simulation tests conducted in Cisco Packet Tracer using the configured network topology, firewall rules, VLAN segmentation and Intrusion Prevention System (IPS) mechanisms discussed in Chapter 4.

Modern research institutions require strong network security frameworks due to the increasing rise in cyber threats targeting intellectual property and confidential organizational data (Moyo & Chikasha, 2023). According to Palo Alto Networks (2025), integrating advanced firewall technologies and intrusion prevention systems significantly improves the ability of organizations to detect and mitigate sophisticated attacks in real time.

5.2 System Implementation Results

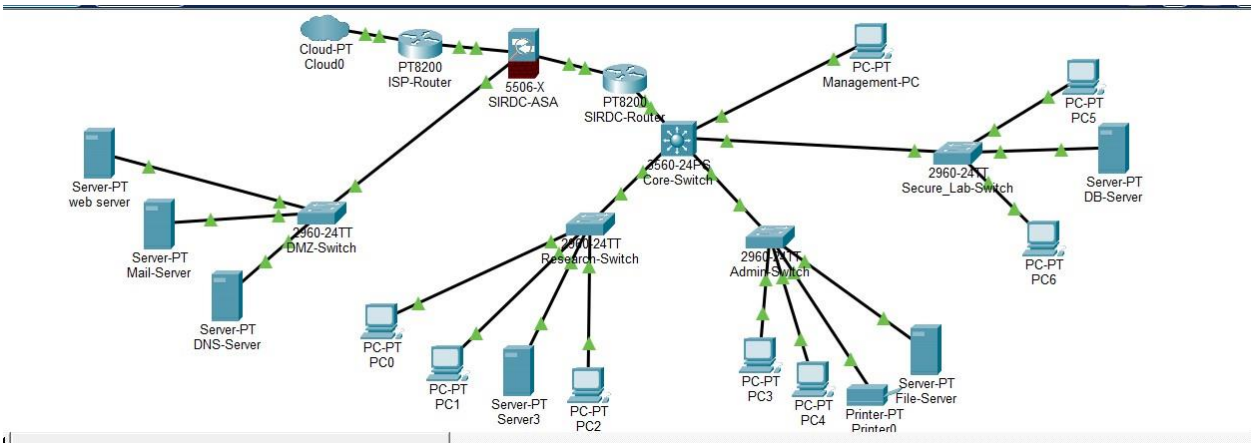
The secure network infrastructure was successfully implemented in a simulated Cisco Packet Tracer environment. The implementation integrated the following key components:

- Firewall security policies
- VLAN segmentation
- Inter-VLAN routing
- Intrusion Prevention System (IPS)
- VPN connectivity
- Access Control Lists (ACLs)
- Network Address Translation (NAT)
- Quality of Service (QoS) mechanisms

The implemented system successfully demonstrated the ability to:

- Block unauthorized external access attempts
- Allow secure communication between authorized VLANs
- Protect sensitive research databases from unauthorized users
- Provide secure remote access through VPN tunnels
- Detect and mitigate suspicious traffic patterns

The implementation aligns with findings by Cisco Systems (2024), which emphasize that simulation-based network testing environments provide effective validation of enterprise security architectures before deployment into production environments. *Fig 5.2 sysytem*



5.3 Network Connectivity Results

Connectivity tests were conducted using ICMP ping requests and HTTP service verification between various network segments. The results confirmed that legitimate communication paths were functioning correctly while unauthorized access was denied according to the configured firewall rules.

Table 5.1: Connectivity Test Results

Source Device	**Destination Device**	**Service Tested**	**Result**
Research PC	Web Server	HTTP	Successful
Research PC	Research Database	ICMP	Successful
Admin PC	Secure Lab Database	ICMP	Blocked
External Attacker PC	Internal LAN	ICMP	Blocked
VPN Client	Research Server	HTTPS	Successful
Internet User	Web Server (DMZ)	HTTP/HTTPS	Successful

The results indicate that the firewall policies effectively enforced the principle of least privilege by allowing only authorized communication between network segments.

This supports the findings of Kabanda (2019), who noted that layered network controls reduce the exposure of sensitive organizational resources to cyber threats.

Fig 5.3 testing valid connection

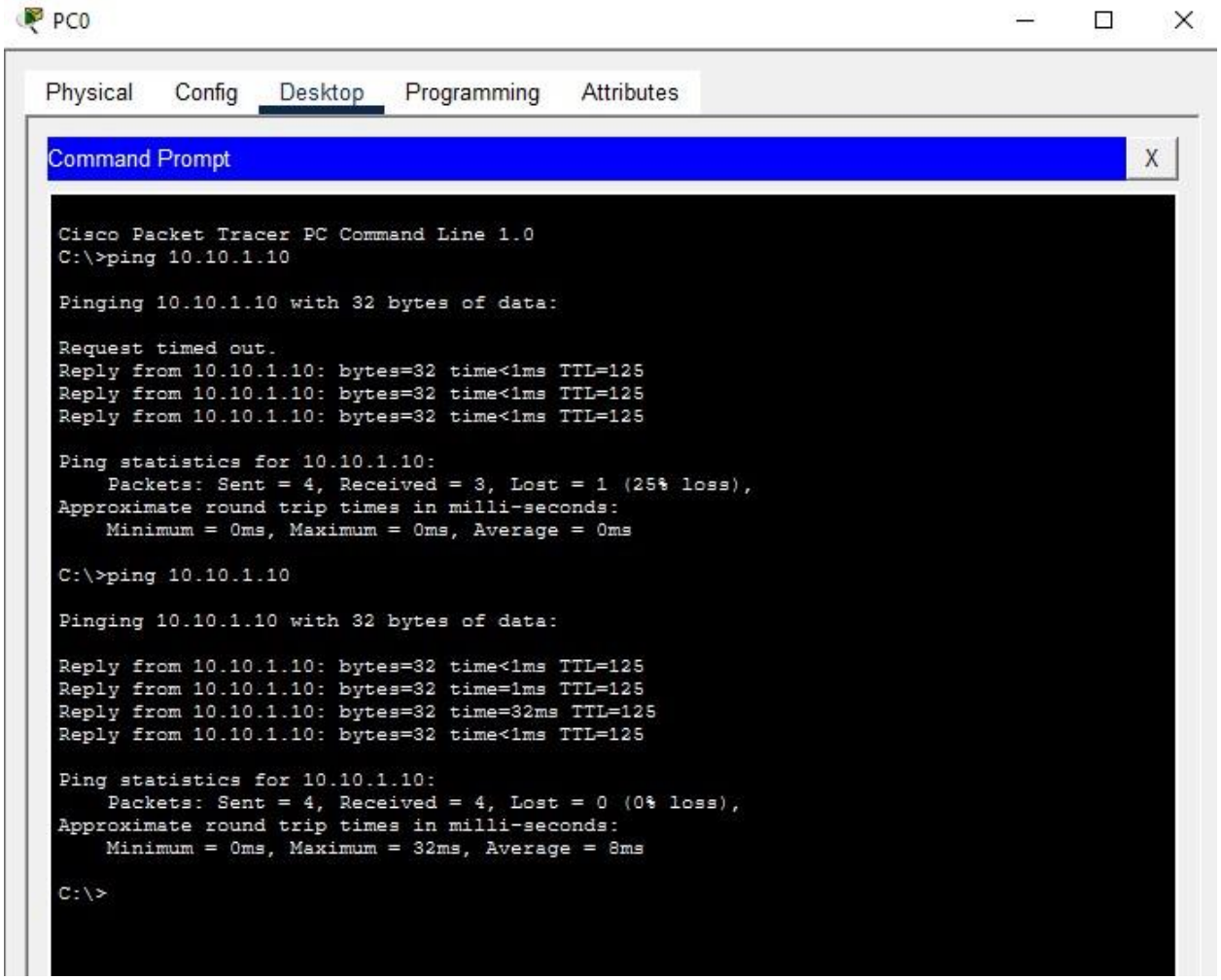


Fig 5.3 testing valid connection

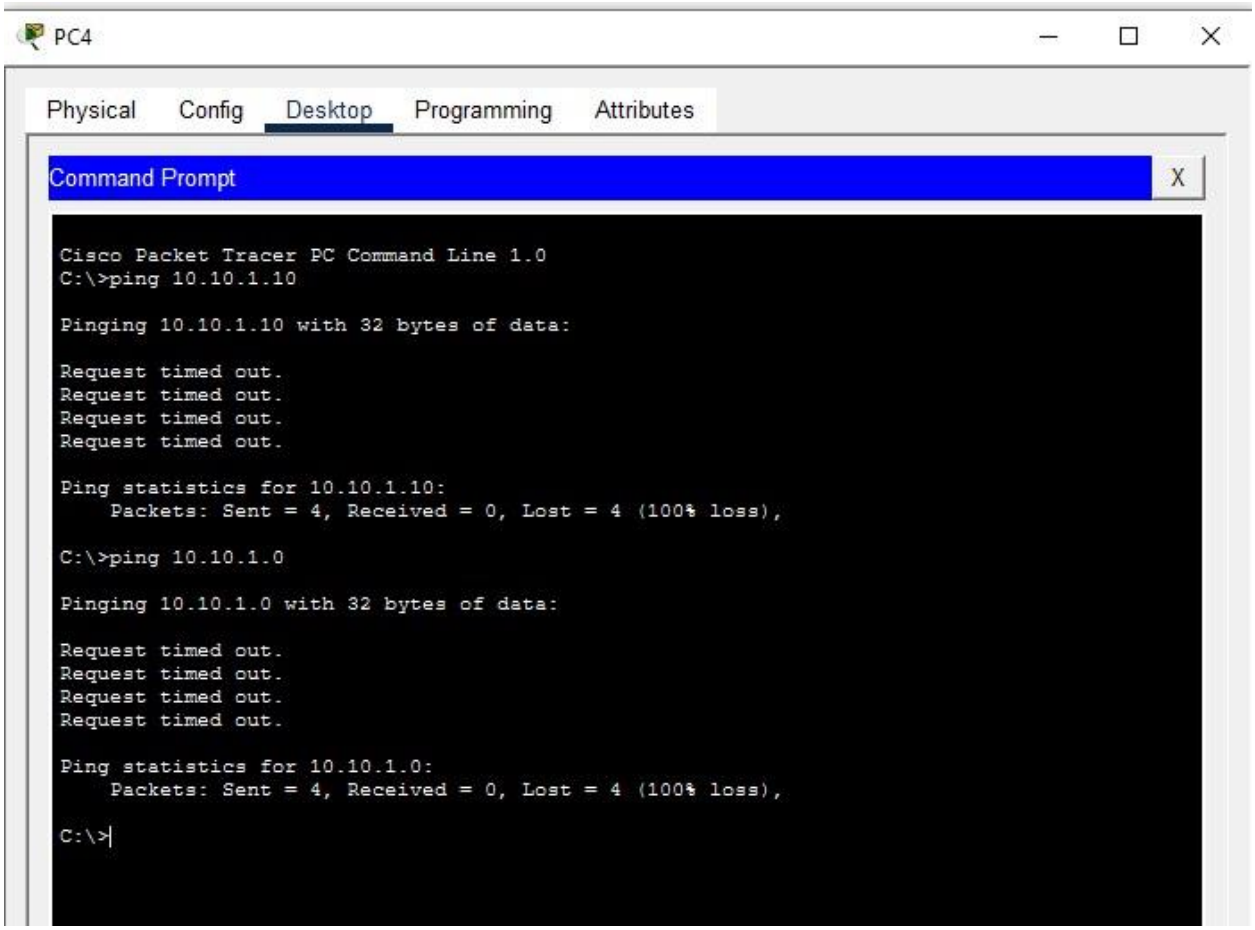


Fig 5.3.1 Invalid connection

5.4 Firewall Performance Results

Firewall testing focused on evaluating traffic filtering accuracy and the prevention of unauthorized access attempts. ACL hit counts and packet inspection logs showed that malicious and unauthorized packets were correctly denied.

Observed Firewall Behaviors

1. All inbound traffic from the internet to the internal LAN was denied by default.
2. Public services hosted in the DMZ remained accessible externally.
3. Unauthorized attempts to access the Secure Lab VLAN were successfully blocked.
4. NAT translation enabled secure internet access for internal users without exposing private IP addresses.

The firewall therefore achieved its intended purpose of isolating sensitive internal resources while maintaining controlled access to public-facing services. Similar findings were highlighted by Mashizha and Kanengoni (2025), who observed that properly configured firewall systems improve institutional cybersecurity resilience and reduce unauthorized access attempts.

5.5 VLAN Segmentation Results

The VLAN segmentation strategy significantly improved network isolation and internal security. Broadcast traffic was reduced and lateral movement between departments was restricted.

Key Findings

- VLAN 20 (Research Network) successfully communicated with approved servers only.
- VLAN 30 (Administrative Network) was isolated from the Secure Lab VLAN.
- VLAN 40 (Secure Lab) remained highly restricted and protected from unauthorized traffic.
- VLAN 99 provided secure management access for administrators only.

The segmentation strategy effectively minimized internal attack surfaces and strengthened departmental isolation. According to Maphosa (2023), network segmentation remains one of the most effective approaches for controlling internal cyber threats and minimizing the spread of attacks within organizations.

Fig 5.5 key findings

```
SIRDC-CoreSW#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/2
10   DMZ                              active
20   Research                         active
30   Admin                            active
40   SecureLab                        active
99   Management                       active    Fa0/5
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
99   enet  100099     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
SIRDC-CoreSW#
```

5.6 Intrusion Prevention System (IPS) Results

The IPS component successfully detected suspicious traffic patterns generated during simulated attack scenarios. Port scanning attempts and abnormal packet flows originating from the simulated attacker device were identified and blocked automatically.

IPS Capabilities Demonstrated

- Detection of suspicious scanning activity
- Automatic dropping of malicious packets
- Logging of unauthorized access attempts
- Real-time traffic inspection

These findings confirm that the integration of IPS functionality improved the network's capability to respond proactively to cyber threats. Manyaya (2024) states that proactive threat detection systems are essential in modern research institutions

due to the increasing sophistication of cyberattacks targeting industrial and scientific data.

5.7 Conclusion

This study successfully achieved its primary objective of designing and implementing a secure network infrastructure for the Scientific and Industrial Research and Development Center (SIRDC). The implemented solution demonstrated the effectiveness of modern firewall technologies, VLAN segmentation and intrusion prevention mechanisms in securing institutional research environments.

The project established that a properly configured firewall system can significantly reduce network vulnerabilities by filtering unauthorized traffic, controlling access between network segments and protecting critical research databases. Furthermore, the implementation of VPN services enhanced secure remote accessibility, while the integration of IPS functionality enabled proactive threat detection and mitigation.

The study also demonstrated the practical applicability of simulation-based testing using Cisco Packet Tracer in validating enterprise network security architectures before real-world deployment (Cisco Systems, 2024). Through the conducted tests and evaluations, the proposed solution proved capable of maintaining confidentiality, integrity and availability within the SIRDC network infrastructure, principles commonly associated with the CIA security model discussed by Moyo and Chikasha (2023).

Overall, the research contributes to the advancement of secure network implementation strategies for research institutions operating in resource-constrained environments such as Zimbabwe.

5.8 Recommendations

Based on the findings obtained during the study, the following recommendations are proposed:

i. Deployment of Enterprise-Grade Hardware

SIRDC should implement the proposed architecture using enterprise-grade firewall appliances and managed switches capable of supporting advanced security services such as Deep Packet Inspection (DPI) and real-time threat analytics. **ii. Continuous Security Monitoring**

The institution should establish a dedicated Security Operations Center (SOC) responsible for continuous monitoring of firewall logs, IPS alerts and suspicious network activities. **iii. Regular Security Audits**

Periodic vulnerability assessments and penetration testing should be conducted to identify emerging weaknesses and ensure that security policies remain effective against evolving threats.

iv. User Awareness Training

SIRDC employees and researchers should undergo regular cybersecurity awareness training to minimize risks associated with phishing, weak passwords and social engineering attacks.

v. System Updates and Patch Management

All network devices, servers and firewall systems should be updated regularly with the latest firmware and security patches to reduce exposure to known vulnerabilities.

vi. Future Integration of AI-Based Threat Detection

Future improvements may include the integration of Artificial Intelligence (AI) and Machine Learning (ML) technologies to automate threat analysis and improve anomaly detection accuracy, as suggested by Palo Alto Networks (2025).

5.9 Summary

This chapter detailed the implementation, analysis and performance evaluation of the proposed secure network architecture for SIRDC. By integrating a robust **firewall system** with **VLAN segmentation**, **Intrusion Prevention Systems (IPS)**, and **VPN technologies**, the results confirmed a substantial strengthening of the network perimeter and a marked reduction in unauthorized access vulnerabilities.

The findings validate that this multi-layered approach effectively mitigates modern cyber threats. Based on these outcomes, the chapter concluded with a synthesis of the study's contributions and offered actionable recommendations to bolster the institution's long-term cybersecurity resilience and guide future infrastructure deployments.

References

Kabanda, S. (2019). Cybersecurity in the developing world*:* A study of the challenges faced by organizations in the SADC region. *Journal of African Information Systems, 11(2), 45-62.*

Manyaya, M. (2024). *The digital frontier: Zimbabwe's transition to the Fourth Industrial Revolution and the rising cyber threat landscape*. Harare: University of Zimbabwe Publications.

Maphosa, V. (2023). Cyber-attack vectors in Zimbabwe: A comprehensive analysis of ransomware and phishing trends. *Zimbabwean Journal of Science and Technology, 18(1), 12-28.*

Mashizha, T., & Kanengoni, R. (2025). *Evaluating the adequacy of network security frameworks in Zimbabwean research institutions.* [Unpublished technical report]. Harare Institute of Technology.

Moyo, T., & Chikasha, S. (2023). Cybersecurity challenges and infrastructure gaps in resourceconstrained environments: A case of Zimbabwe. *International Journal of Computer Science and Network Security, 23(4),* 101-115.

Palo Alto Networks. (2025). *The state of network security: Navigating the blind spots of encrypted SSL/TLS traffic.* White Paper. Retrieved from https://www.paloaltonetworks.com/resources/whitepapers/state-of-network-security

Zimbabwe Government. (2021). *Cyber and Data Protection Act [Chapter 12:07]*. Harare: Government Printer

Cisco Systems. (2024). *Cisco Packet Tracer (Version 8.2)* [Computer software]. Cisco Networking Academy. https://www.netacad.com/courses/packet-tracer

Liquid Intelligent Technologies. (2025, August 26). *Security first: Becoming a threat-resilient organisation in Zimbabwe.* https://liquid.tech/cyber-security-resilience-in-zimbabwe/

APPENDICES

Appendix A: Network Security Questionnaire

BINDURA UNIVERSITY OF SCIENCE EDUCATION — Department of Computer Science

Study Title: Scientific & Industrial Research and Development Center (SIRDC) Secure Network

Researcher: Method Ndeya B221451B

Supervisor: ____ Mr Chituma____

Instructions

This questionnaire is intended for ICT personnel, network administrators, researchers and staff members at the Scientific and Industrial Research and Development Center (SIRDC). The purpose of this study is to assess network security challenges and evaluate the effectiveness of secure network solutions within the institution. All responses will remain confidential and will be used strictly for academic purposes.

SECTION A: RESPONDENT PROFILE

A1. What is your role at SIRDC?

□ Network Administrator

□ ICT Technician

□ Research Staff

□ Administrative Staff

□ Management

□ Other: _____

A2. How many years of experience do you have working with computer networks or ICT systems?

□ Less than 1 year

□ 1–3 years

□ 4–6 years

□ 7–10 years

□ More than 10 years

A3. What is your highest level of education?

□ Certificate / Diploma

□ Bachelor's Degree

□ Master's Degree

□ Doctorate Degree

□ Other: _____

SECTION B: CURRENT NETWORK SECURITY STATUS

B1. How would you rate the current network security at SIRDC?

□ Very Poor

□ Poor

□ Average

□ Good

□ Excellent

B2. Have you ever experienced any of the following network-related problems at SIRDC? (Tick all that apply)

□ Unauthorized access attempts

□ Malware or virus attacks

□ Slow network performance

□ System downtime

□ Phishing emails

□ Data loss incidents

□ Ransomware attacks

□ None of the above

B3. How often does the organization experience network downtime or security-related disruptions?

□ Daily

□ Weekly

□ Monthly

□

Rar

ely

□

Ne

ver

B4. Are current firewall and security systems effective in preventing unauthorized access?

□ Strongly Agree

□ Agree

□ Neutral

□ Disagree

□ Strongly Disagree

B5. How satisfied are you with the current network monitoring and security tools?

□ Very Dissatisfied

□ Dissatisfied

□ Neutral

□ Satisfied

□ Very Satisfied

SECTION C: FIREWALL AND NETWORK SECURITY IMPLEMENTATION

C1. Which of the following security technologies are currently used at SIRDC? (Tick all that apply)

□ Firewall

□ VPN

□ Intrusion Prevention System (IPS)

□ Antivirus Software

□ Access Control Lists (ACLs)

□ VLAN Segmentation

□ Network Monitoring Tools

□ Not Sure

C2. Do you believe VLAN segmentation improves internal network security?

□ Strongly Agree

□ Agree

□ Neutral

□ Disagree

□ Strongly Disagree

C3. How important is secure remote access (VPN) to SIRDC operations?

□ Very Important

□ Important

□ Neutral

□ Less Important

□ Not Important

C4. What are the biggest challenges affecting network security at SIRDC? (Tick all that apply)

□ Limited security budget

□ Lack of modern equipment

□ Weak password practices

□ Lack of staff awareness

□ Increasing cyber threats

□ Poor internet reliability

□ Inadequate monitoring systems

□ Other: _____

C5. What improvements would you recommend for strengthening network security at SIRDC?

Thank you for your participation.

Appendix B: Key Informant Interview Guide

BINDURA UNIVERSITY OF SCIENCE EDUCATION — Department of Computer Science

Study Title: Scientific & Industrial Research and Development Center (SIRDC) Secure Network

Researcher: Method Ndeya B221451B

Target Respondents

- ICT Managers
- Network Engineers
- System Administrators
- Technical Staff at SIRDC

Expected Duration

20–30 Minutes

Preamble

Good morning/afternoon. My name is Method Ndeya, a final-year student at Bindura University of Science Education studying Network Engineering. I am conducting research on the implementation of a Secure Network Infrastructure for SIRDC. The interview aims to gather professional insights regarding network security challenges, firewall implementation and cybersecurity management. Your responses will remain confidential and will only be used for academic purposes.

THEME 1: CURRENT NETWORK INFRASTRUCTURE

1. Can you describe the current network infrastructure at SIRDC?

Probes:

- *Number of connected devices*
- *Existing internet connectivity*

- *Current firewall solutions*
- *Server infrastructure*

2. What are the major cybersecurity threats currently affecting the organization?

Probes:

- *Malware attacks*
- *Unauthorized access attempts*
- *Phishing attacks*
- *Insider threats*

3. How does the organization currently monitor and manage network traffic?

Probes:

- *Existing monitoring tools*
- *Log analysis methods*
- *Incident response procedures*

THEME 2: FIREWALL IMPLEMENTATION AND NETWORK SECURITY

4. How effective are the current firewall systems in protecting the organization's network?

Probes:

- *Traffic filtering*
- *Access control effectiveness*
- *Detection of malicious traffic*

5. What challenges are encountered in maintaining secure network operations?

Probes:

- *Hardware limitations*
- *Budget constraints*
- *Lack of skilled personnel*
- *User negligence*

6. How important is VLAN segmentation in protecting sensitive organizational resources?

Probes:

- *Departmental isolation*
- *Internal traffic control*
- *Limiting lateral movement*

THEME 3: VPN, IPS AND THREAT MANAGEMENT

7. How effective is the current remote access system used by SIRDC?

Probes:

- *VPN usage*
- *Remote authentication*
- *Data encryption effectiveness*

8. What role does Intrusion Prevention Systems (IPS) play in securing the network?

Probes:

- *Threat detection capabilities*
- *Real-time response*
- *Attack prevention success rates*

9. How prepared is the institution to respond to future cyber threats?

Probes:

- *Staff training*
- *Security awareness programs*
- *Disaster recovery strategies*

THEME 4: RECOMMENDATIONS AND FUTURE IMPROVEMENTS

10. What improvements would you recommend for strengthening SIRDC's network security infrastructure?

Probes:

- *Advanced firewall technologies*
- *AI-based threat detection*
- *Cloud security integration*
- *Security policy enhancements*

11. Is there anything else you would like to share regarding cybersecurity management at SIRDC?

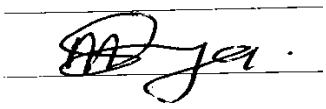
Thank you for your time and valuable contribution.

Appendix C: Signed Research Proposal

[Please insert the signed research proposal document here. The proposal should bear the signatures of the student researcher (Method Ndeya, B221451B) and the academic supervisor, together with the approval stamp or endorsement from the Department of Computer Science, Bindura University of Science Education.]

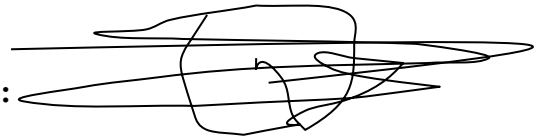
Student Name: Method Ndeya (B221451B)

Research Topic: *Scientific & Industrial Research and Development Center (SIRDC) Secure Network*



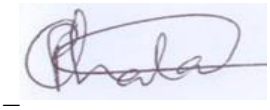
Student Signature: ___ _____

Date: _____23/06/2026**_____**



Supervisor Signature:

Date: ___23/06/2026**_____**



Chairperson / HOD Signature: _

Date: ___23/06/2026**____**



Departmental Stamp / Approval: ___

Date: __23/06/2026_____