

**Final Year Design Project Proposal Document**

**VPN SpyGlass: VPN traffic analyzer**

By

Hassan Abdullah 337275

Sameen Mubashar 346848

**Supervisor:**

Dr. Mehdi Hussain

**Co-Supervisor*:***

Dr*.* Arsalan Ahmad

**Bachelor of Science in Computer Science**

**(2020-2024)**

Department of Computing

School of Electrical Engineering and Computer Science

National University of Sciences & Technology

# ABSTRACT

The "VPN SpyGlass" project intends to develop a VPN traffic analyser tool that can improve network security by detecting and assessing VPN activities. The programme uses deep packet inspection techniques to distinguish between VPN and conventional network traffic and provides real-time monitoring via a customisable internet dashboard. The project solves VPN-related obstacles, such as security risks, privacy concerns, and network performance issues, by providing a comprehensive solution for effective network security management.

# INTRODUCTION

The usage of VPNs is expanding as people become more concerned about their online privacy and security, as well as the desire to go around geo-restrictions and access region-specific material. **Controlling** **VPN** **use**, on the other hand, is critical for **preventing security concerns by monitoring and controlling encrypted traffic, protecting against possible misuse, optimizing network performance, and ensuring compliance with network policies and laws**. **Deep packet analysis is critical for comprehending network traffic** (Figure 1) since it inspects individual data packets, allowing for better security monitoring, threat detection, and network optimization. However, there has been little study towards identifying internal application activity via encrypted network traffic, particularly for VPNs. There is a dire need to research encryption solutions for today's cutting-edge network traffic for analysis and inspection.

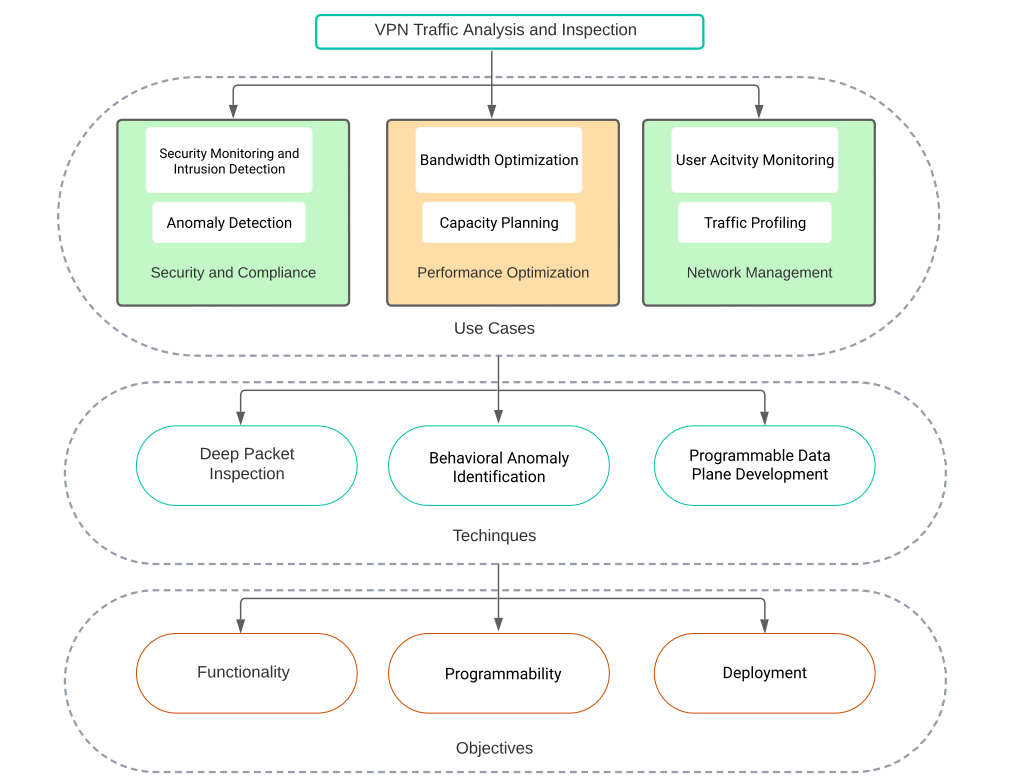


Figure 1

The purpose of this research is to **look into the encrypted network traffic used by VPN providers to determine the traffic pattern, protocol identification, and participating servers**. The proposed methodology will capture traffic using a P4 Switch, as shown in Figure 2. Various VPNs will be installed on devices and linked to the internet through a wireless access point passing through switch. To filter out the corresponding apps, all internet traffic from the wireless access point will be routed through the P4 switch and information will be forwarded to the controller. Wireshark and other cutting-edge tools will be used to monitor encrypted data via trace file analysis for network traffic monitoring. The IP addresses, ports, packet lengths, and packet patterns will be utilized to identify the VPN and the exact VPN that is being used. It is worth mentioning that the IP addresses and ports are in plaintext, however the payloads are encrypted for the purpose of secrecy and privacy. The knowledge gathered from this study will aid in the **building of a Network Traffic Analysis for VPNs, as well as the ability to block VPN in a specific network.**

A diagram of a computer network

Description automatically generated

The project targets the issues that consumers have while navigating the VPN sector, with the goal of providing clear, unbiased information and tools to assist users in making educated VPN service selection decisions. By integrating robust network analysis with user-friendly interface design, the project allows users to control VPN usage, improve network security, and increase network visibility. The purpose is to enable network administrators to identify unauthorised VPN connections, categorise VPN traffic, and reduce security risks by leveraging modern technology and deep packet inspection algorithms.

# PROBLEM STATEMENT

 “The proliferation of VPNs poses a challenge to network admin, as these tools can bypass security measures and access restricted content pose security risks, violate agreements, and slow network performance. Moreover, Existing methods often struggle to identify VPN traffic due to encryption and masking techniques employed by VPN services.”

# PROJECT OVERIEW/GOAL

|  |
| --- |
| * Acquire a thorough comprehension of the analysis of encrypted network traffic. * The goal of this study is to look into the difficulties in examining network traffic that has been tunneled or encrypted. * Recognize and investigate the many applications and use cases for encrypted traffic analysis. |

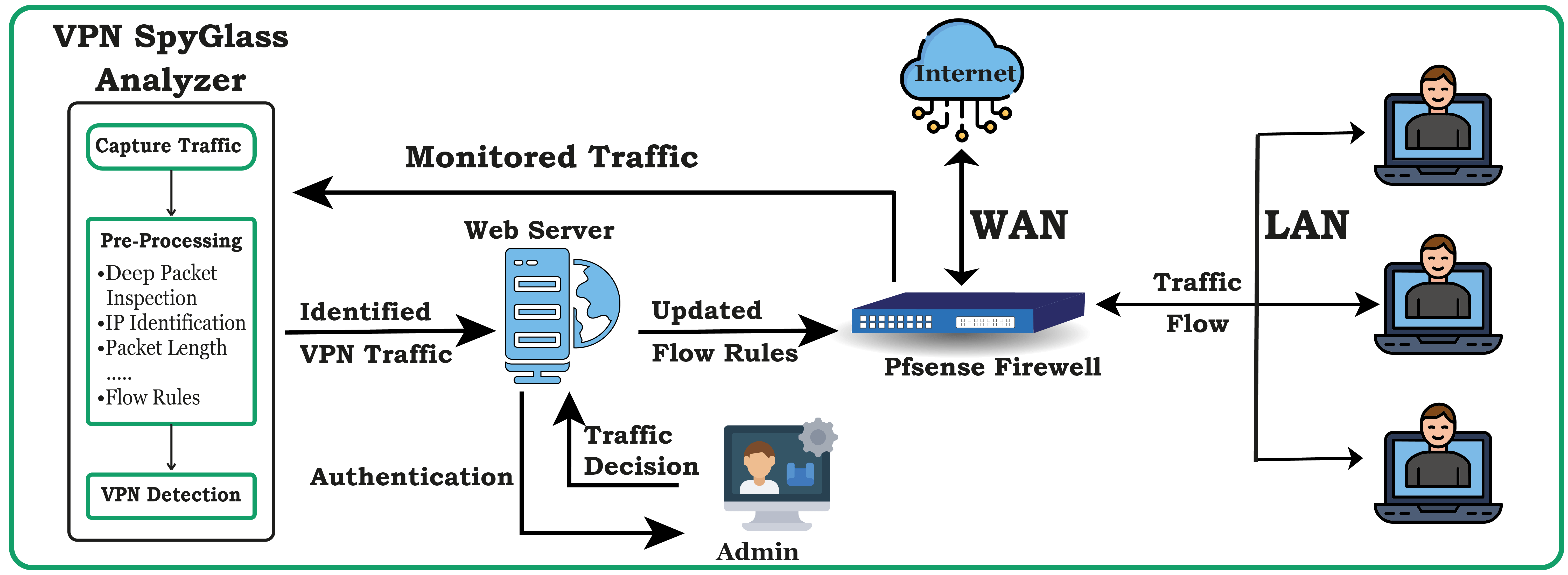
## Outcomes of the FYP:

|  |
| --- |
| * 1x high-quality publication * A straightforward encrypted network traffic analysis module capable of distinguishing between VPN and conventional traffic as well as particular VPN types. * A web interface that provides real-time traffic analysis and allows us to disable VPN connections in a specified network. |

# PROJECT DEVELOPMENT METHODLOGY / ARCHITECTURE

## Overall Architecture

The project's aims are divided into smaller objectives/modules, such as online dashboard creation, cloud database integration, hosting setup, and classification algorithm implementation. The system design consists of ReactJS/NextJS for the online interface, NodeJS for backend services, and Python for classification algorithms. The project process is agile, enabling flexibility and response to change requirements.



## Research Architecture

For Research Architecture, use the following structure.

|  |
| --- |
|  |

In this way, you are able to capture the traffic on the laptop – User A so that you can perform Deep Packet Inspection.

# Future Work

There are multiple suggestions for future work. Some of them are as follows:

1. Implement blocking using OpenFlow Rules or P4 Switches
2. Automate the Detection Process for new VPNs or change in characteristics of an existing VPN.
3. Automate the Blocking Part of the Project.
4. Perform DPI to Identify what activity is being performed or what sites are being visited while the VPN is active.
5. Study Behavior of VPN in different environments like Proxy, VPN followed by Proxy, Proxy followed by VPN, VPN in a virtual Box and VPN along with Tor Browers, etc., just to name a few.