VPN SpyGlass
VPN Traffic Analyzer

Introduction

VPN SpyGlass is an open-source tool that detects and categorizes VPN traffic on a network using deep packet inspection. Identifying VPN traffic is difficult due to encryption and masking techniques used by VPN services. VPN SpyGlass classifies VPN traffic by protocol or type, aiding network administrators in monitoring and managing VPN usage, identifying unauthorized connections, tracking user activity, and uncovering security risks.

Objective

1. Conduct deep packet inspection of encrypted traffic to pinpoint VPN usage patterns.
2. Create rapid and precise ways for detecting encrypted VPN traffic, allowing for immediate reaction to security threats.
3. Create a user-friendly VPN analyzer application with admin controls, allowing admin to properly oversee and regulate VPN usage.

Features

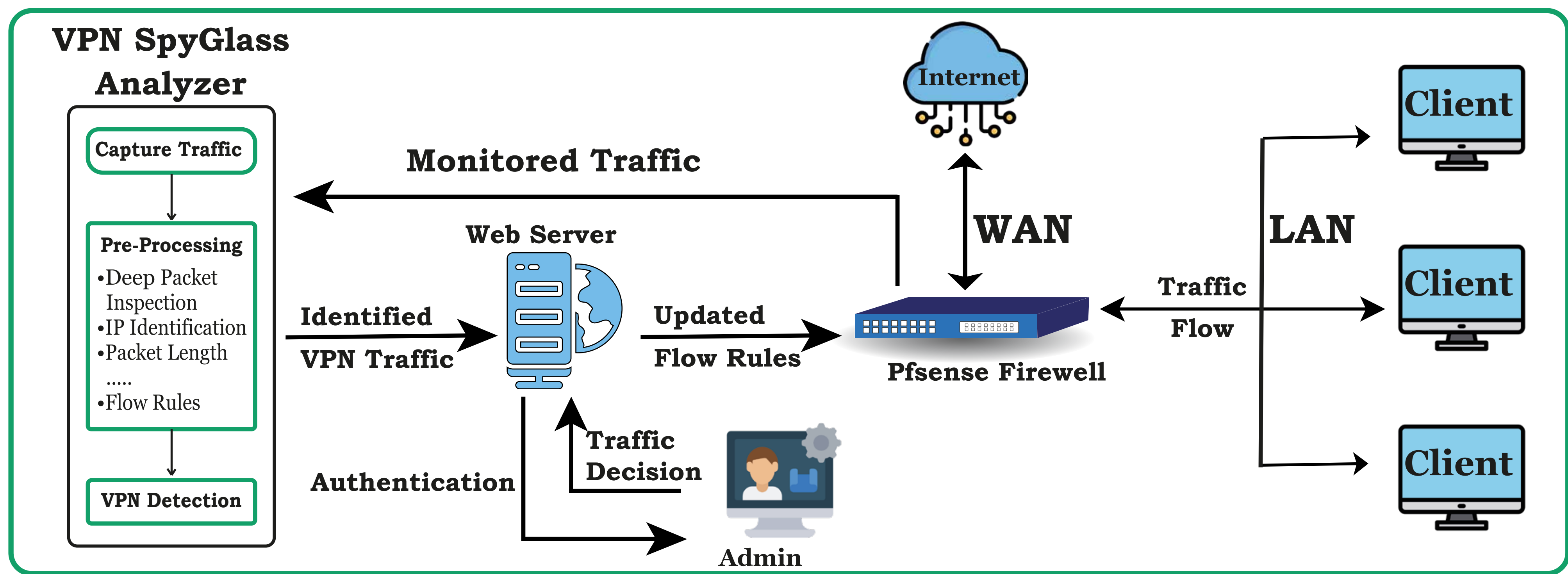| Live Analytic Dashboard | VPN Traffic Categorization | Network Control | Notification Alerts | User Authentication & Access Control |

System Architecture

VPN SpyGlass Analyzer — Capture Traffic → Pre-Processing (•Deep Packet Inspection •IP Identification •Packet Length ..... •Flow Rules) → VPN Detection. Identified VPN Traffic → Web Server → Updated Flow Rules → Pfsense Firewell. Monitored Traffic. Authentication. Traffic Decision → Admin. Internet — WAN. Pfsense Firewell — Traffic Flow — LAN → Client, Client, Client.

Outcome

• Identify VPN Traffic
• Identify VPN Application
• Identify VPN Ports and IP Addresses
• Blocking VPN usage in network using PfSense

Conclusion

Compared to traditional methods, VPN SpyGlass provides more control to the system administrator to detect and restricted use of VPN in a network.
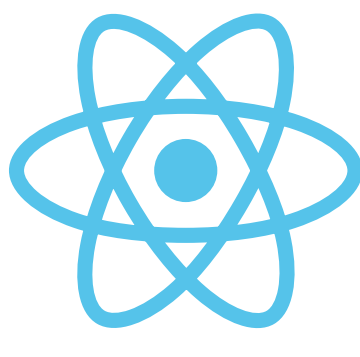Research Paper Submitted in "Confrence Name"

Technologies

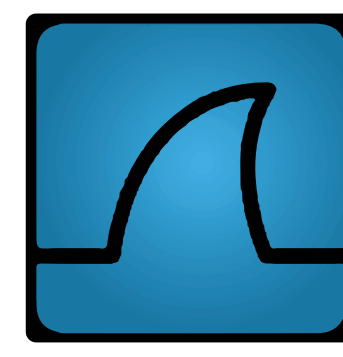| Python | NodeJs | ReactJs | PfSense | WireShark | MongoDB Atlas |

Group Members

Hassan Abdullah
Sameen Mubashar

Advisor: Dr. Medhi Hussain
Co-Advisor: Dr. Arsalan Ahmad