

**User Guide**

**VPN SpyGlass: VPN traffic analyzer**

By

Hassan Abdullah 337275

Sameen Mubashar 346848

Table of Contents

[USER GUIDE iii](#_Toc166018456)

[1.1 Project Overview iii](#_Toc166018457)

[1.2 Overview of modules iii](#_Toc166018458)

[VPN SpyGlass Installation and Setup Guide iv](#_Toc166018459)

[Step 1: Download Node.js iv](#_Toc166018460)

[Step 2: Clone the Repository iv](#_Toc166018461)

[Step 3: Set up the Frontend iv](#_Toc166018462)

[Step 4: Set up the Backend iv](#_Toc166018463)

[Step 5: Configure Backend v](#_Toc166018464)

[Step 6: Run the Backend Server v](#_Toc166018465)

[Downloading and connecting to MongoDB Compass v](#_Toc166018466)

[Step 1: Download MongoDB Compass v](#_Toc166018467)

[Step 2: Launch MongoDB Compass v](#_Toc166018468)

[Step 3: Connect to MongoDB Atlas v](#_Toc166018469)

[Step 4: Enter Connection Details vi](#_Toc166018470)

[Step 5: Test Connection and Connect vi](#_Toc166018471)

[Step 6: Explore and Manage Your Data vii](#_Toc166018472)

[Capturing Network Traffic with Python Script vii](#_Toc166018473)

[Step 1: Clone the Repository vii](#_Toc166018474)

[Step 2: Open Folder vii](#_Toc166018475)

[Step 3: Verify Working vii](#_Toc166018476)

[PfSense Firewall Installation and Setup Guide vii](#_Toc166018477)

[Step 1: Download PfSense Firewall vii](#_Toc166018478)

[Step 2: Download Rufus viii](#_Toc166018479)

[Step 3: Install PfSense Installer on USB viii](#_Toc166018480)

[Step 4: Installing PfSense ix](#_Toc166018481)

[Step 5: Configure PfSense ix](#_Toc166018482)

[PfSense Firewall Rule Management for Network Traffic Control ix](#_Toc166018483)

[Step 1: Open Admin Panel ix](#_Toc166018484)

[Step 2: Setting up Firewall Rules ix](#_Toc166018485)

# USER GUIDE

Welcome to the VPN Spyglass User guide.

This guide covers all of VPN Spyglass’s functionalities from a user’s perspective.

## Project Overview

The "VPN SpyGlass" project develops a unique VPN traffic analysis tool that enhances network security by utilizing deep packet inspection techniques to separate VPN activity from regular network traffic. With real-time monitoring via a dynamic internet dashboard, it tackles VPN-related challenges such as security threats, privacy difficulties, and network performance problems, offering a full solution for effective network security management. Customers' worries while navigating the VPN environment drive its robust grading criteria and user-friendly interface, which make it possible for users to make informed judgments about VPN services and increase online privacy and security. VPN SpyGlass enhances network administrators' ability to recognize unwanted VPN connections, classify VPN traffic, and lessen security hazards by fusing advanced network analysis with an intuitive user interface. This helps to foster a more secure online environment.

## Overview of modules

The VPN SpyGlass project's flexible technology stack is made up of several key components that have been meticulously developed for efficient network security control. Essentially, the Web Dashboard uses Vite, Typescript, and React.js to offer a seamless user experience, while Firebase Servers are utilized to handle data reliably. It ensures that Node.js and Express.js are powering reliable backend operations using Postman for simpler API testing and MongoDB Atlas for cloud database administration. Its advanced Python classifiers based on Deep Packet Inspection (DPI) enable precise separation of VPN data from regular network traffic. PfSense Firewall is linked with network control functions developed in Python to enhance network administration and monitoring. Following are the components of our project along with the tech stack.

|  |  |
| --- | --- |
| **Component** | **Technologies Used** |
| Web Dashboard | React Js  Vite  Typescript  Servers |
| Cloud Database | Mongodb Atlas  PostMan  Node Js  Express Js |
| Hosting | Vercel app |
| Categorization Algorithms | DPI  Python |
| Network Control | Python  PfSense Firewall |

# VPN SpyGlass Installation and Setup Guide

Thank you for choosing VPN SpyGlass for your network security management needs. Below are the steps to get started with cloning the repository, setting up the frontend and backend, and running the application.

## Step 1: Download Node.js

If you haven't already installed Node.js on your system, please download and install it from [here](https://nodejs.org/).

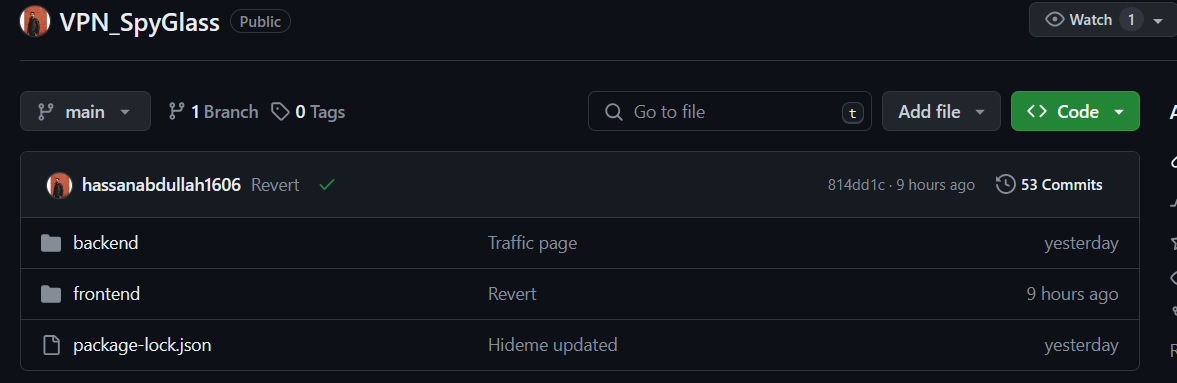
## Step 2: Clone the Repository

Open Visual Studio Code (VS Code) and navigate to the terminal.

Use the following command to clone the repository:

*git clone* [*https://github.com/hassanabdullah1606/VPN\_SpyGlass.git*](https://github.com/hassanabdullah1606/VPN_SpyGlass.git)

The directory structure of the project is as follows:



## Step 3: Set up the Frontend

Navigate into the `frontend` directory:

*cd frontend*

Install the required dependencies by running:

*npm install*

If you haven't installed Firebase, please download and install it by running:

*npm install firebase*

To run the frontend on the development server, execute:

*npm run dev*

## Step 4: Set up the Backend

Navigate into the `backend` directory into separate terminal:

*cd backend*

Install the required dependencies by running:

*npm install*

Additionally, install Express.js and Mongoose by running:

*npm i express mongoose*

## Step 5: Configure Backend

Create a `.env` file in the `backend` directory and add your MongoDB database link to the `DB\_URI` variable:

**DB\_URI**="mongodb+srv://habdullahbscs20seecs:1Zj4MxA3Sv44xzPJ@vpnspyglass.yg51vbe.mongodb.net/?retryWrites=true&w=majority&appName=VPNSpyGlass"

## Step 6: Run the Backend Server

To start the backend server, execute:

node server.js

Congratulations! You have successfully set up VPN SpyGlass on your system.

# Downloading and connecting to MongoDB Compass

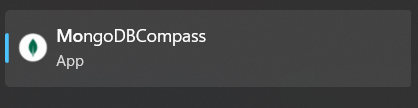
Below are the steps to get started with MongoDB Compass.

## Step 1: Download MongoDB Compass

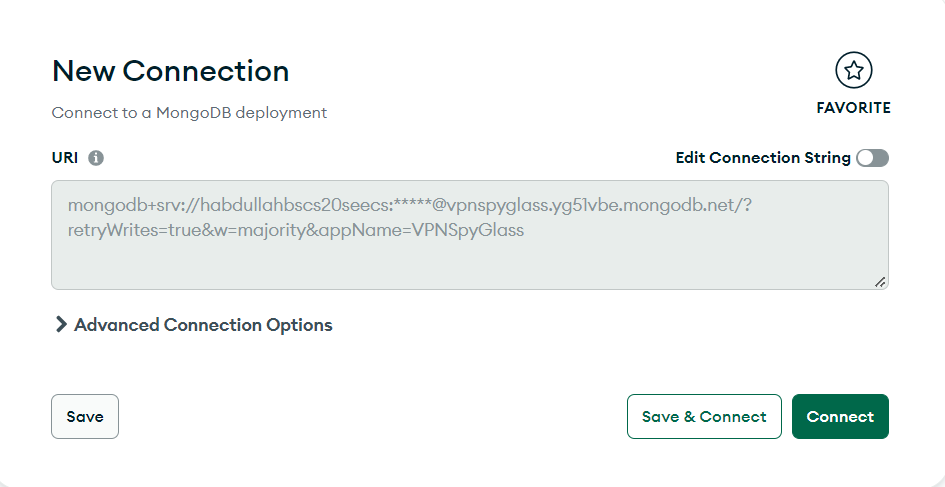
Visit the [MongoDB Compass download page](https://www.mongodb.com/try/download/compass) and download the appropriate version of MongoDB Compass for your operating system (Windows, macOS, or Linux).Follow the installation instructions to complete the installation process.

## Step 2: Launch MongoDB Compass

After installing MongoDB Compass, launch the application from your desktop or applications folder.



## Step 3: Connect to MongoDB Atlas

Upon launching MongoDB Compass, you'll be prompted to connect to a MongoDB instance. Choose the "Connect to" option, and then select "Connect to MongoDB Atlas".

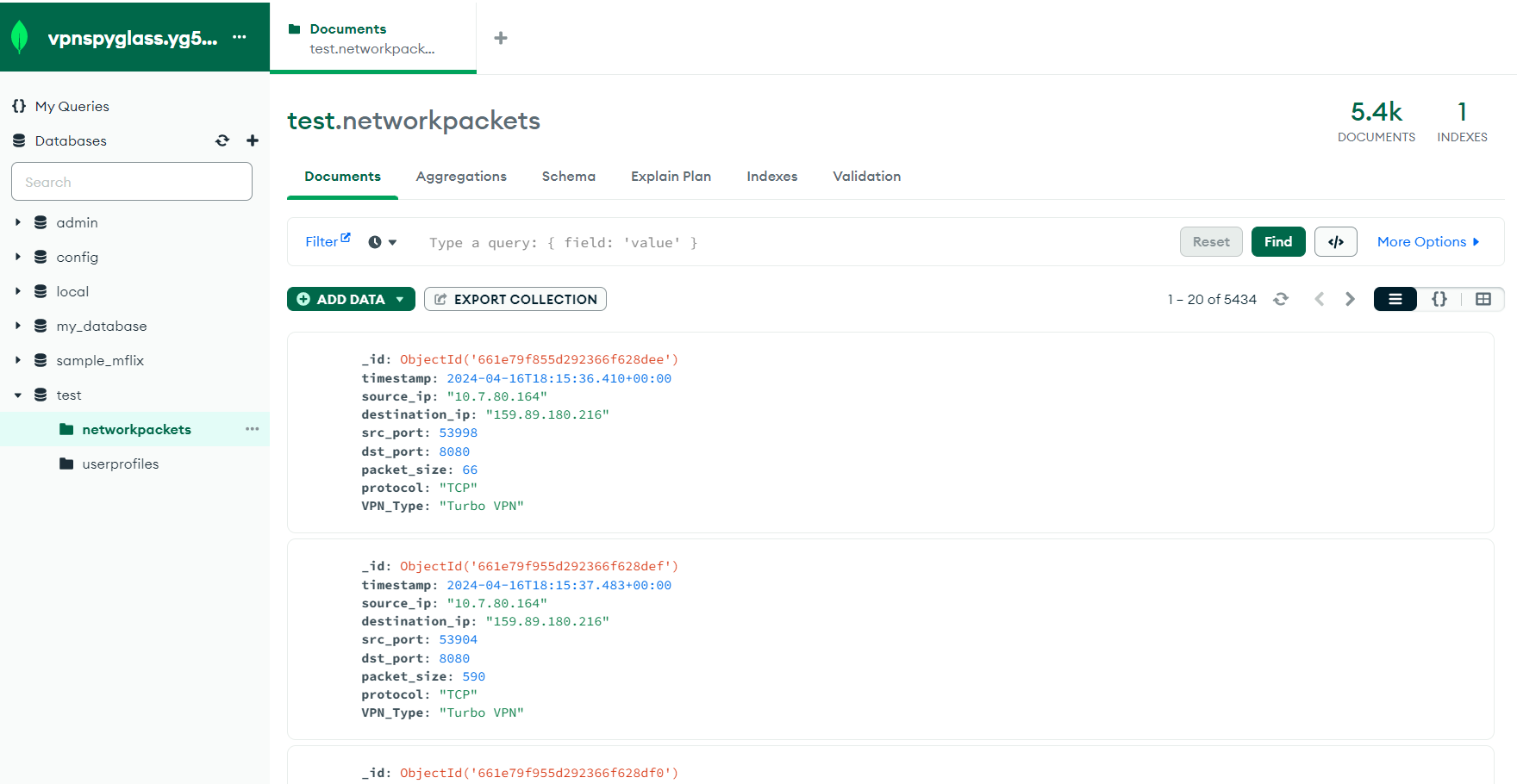
## Step 4: Enter Connection Details

In the connection dialog box, you'll need to enter your connection details. Paste the DB\_URI connection string into the "Connection String" field. It should look something like this:

*"mongodb+srv://habdullahbscs20seecs:1Zj4MxA3Sv44xzPJ@vpnspyglass.yg51vbe.mongodb.net/?retryWrites=true&w=majority&appName=VPNSpyGlass"*

## Step 5: Test Connection and Connect

After entering the connection details, click the "Connect" button to test the connection. If the connection is successful, MongoDB Compass will display a list of available databases and collections in your MongoDB Atlas cluster.



## Step 6: Explore and Manage Your Data

Once connected, you can explore your databases and collections, view documents, perform queries, and manage your data using the intuitive interface of MongoDB Compass.

Congratulations! You have successfully downloaded and connected to MongoDB Compass using the provided DB\_URI key. You can now use MongoDB Compass to interact with your MongoDB Atlas cluster and manage your data effectively.

# Capturing Network Traffic with Python Script

## Step 1: Clone the Repository

Open Visual Studio Code (VS Code) and navigate to the terminal.

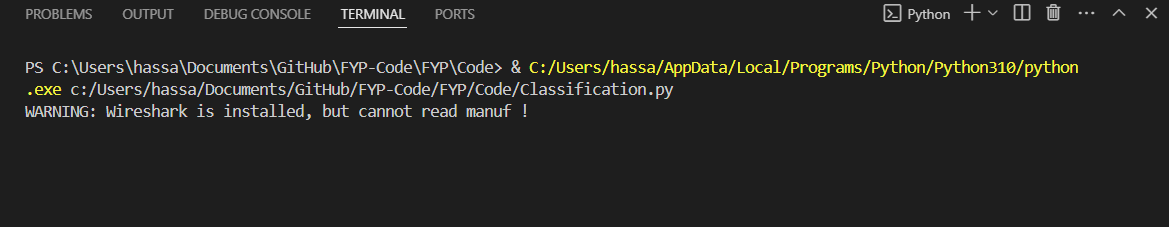
Use the following command to clone the repository:

*git clone* [*https://github.com/hassanabdullah1606/FYP-Code.git*](https://github.com/hassanabdullah1606/FYP-Code.git)

## Step 2: Open Folder

Open VS Code and navigate to the folder “FYP/Code”.

In this folder, run the file named “Classification.py” by pressing on the run python file button. You’ll see the following output on the terminal.



## Step 3: Verify Working

Turn on a VPN on your network and check for new entries in the mongo DB Compass. If new entries are present, then the script is working correctly. Otherwise, change the interface (*identify\_vpn\_live(interface="Ethernet") Line 236*).

# PfSense Firewall Installation and Setup Guide

Install PfSense Firewall on a system that is available.

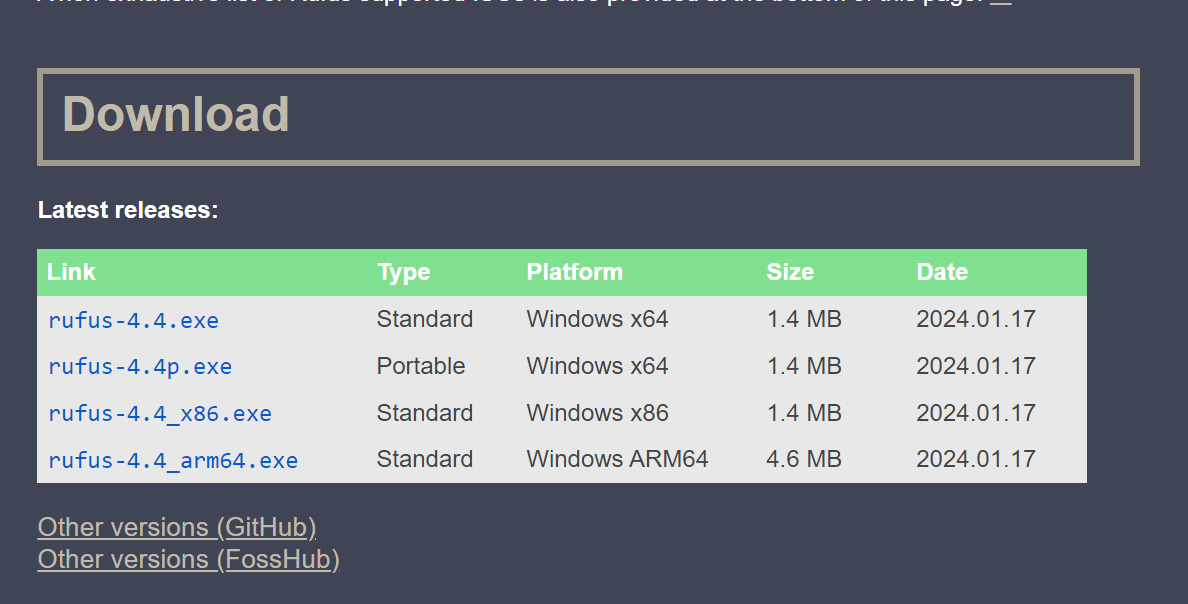
## Step 1: Download PfSense Firewall

Visit [PfSense Firewall community](https://www.pfsense.org/download/) page and download the Latest version of CE-memstick- serial from the website.



## Step 2: Download Rufus

Visit [Rufus download](https://rufus.ie/en/) page and download the Latest version of rufus software from the website.



## Step 3: Install PfSense Installer on USB

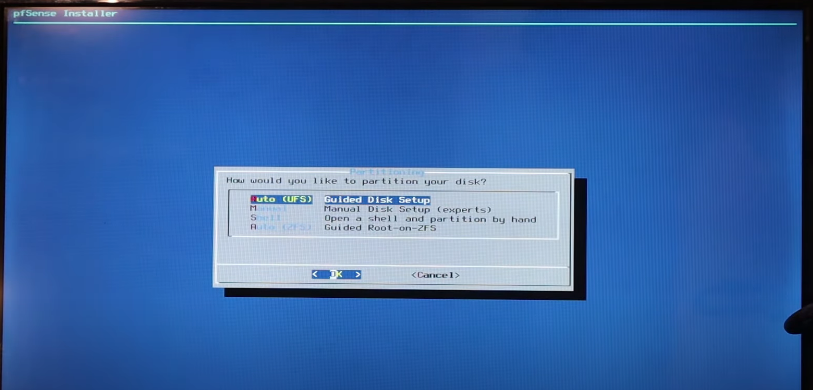
Insert your USB in your system and open Rufus app. Select the downloaded PfSense Installer and the USB stick, and then click on **start** to burn on USB. It will convert the USB stick to a Bootable PfSense installer.

A screenshot of a computer

Description automatically generated

## Step 4: Installing PfSense

On your old System, plug in your USB and power on the system. Press F2 (Depending on the system you are using) as soon as the system boots to enter the boot menu. In the boot menu, select the FreeBSD to start the installer. Once the installer starts, select the “Auto (USF)” option.

****

Now, write on the entire disk. It will format the whole system and only the PfSense will be installed.

**A computer screen with a message

Description automatically generated**

## Step 5: Configure PfSense

You can complete the setup using the following [tutorial video](https://www.youtube.com/watch?v=YD23HSfzq1E).

# PfSense Firewall Rule Management for Network Traffic Control

## Step 1: Open Admin Panel

In your admin system, connected to the PfSense, open a browse, and enter “192.168.1.1”. It will open the PfSense admin dashboard. The credentials are as:

**Username**: *admin*

**Password**: *pfsense (Default)*

Use the password you have set in step 5: Configure PfSense.

## Step 2: Setting up Firewall Rules

Go to Firewall -> Rules.

Click on “LAN”.

It will take you to LAN rules. There you can add blocking rules according to your need. Normal practice is to set the host system as “LAN Subnet” in Source or Destination.