|  |
| --- |
| Cos 301 capstone Project |
| Denendr User Manual |
| [Type the document subtitle] |
| Ruslynn Appana  Jeandre Botha  Muhammed Carrim |
| Sisa Khoza  Christiaan Opperman |
|  |

|  |
| --- |
|  |





Table of Contents

[1. Introduction 3](#_Toc9528708)

[1.1. System Overview 3](#_Toc9528709)

[1.2. System Configuration 3](#_Toc9528710)

[1.3. Installation 3](#_Toc9528711)

[2. Getting started 3](#_Toc9528712)

[3. Using the System 3](#_Toc9528713)

[3.1. Sign in window 3](#_Toc9528714)

[3.2. Home window 3](#_Toc9528715)

[3.3. IP list window 4](#_Toc9528716)

[3.4. Log window 4](#_Toc9528717)

[4. Troubleshooting 4](#_Toc9528718)

# Introduction

## System Overview

The purpose of this system is to protect third party applications from malicious users. The system implements this by detecting DDOS attacks and dropping the packets that are associated with an attack. It also provides load balancing features to control the load for each pool of resources that it is connected to.

The user interacts with the system via an intuitive graphical user interface where the user can to add and remove IP addresses to a white- and blacklist, see packets that traversed the system, view metrics (such as drop rates, packet sizes etc.) and remove and add back-end applications.

## System Configuration



Request

Defendr Server



Request Forward

Answer

Third party’s client

Servers

There are three main components in this system, namely: servers on which back-end applications run, normal devices that the client uses to connect to the third party application and a server on which Defendr executes. The servers on which back-end applications run and the normal devices that the client uses to connect to the third party application is beyond the scope of this user manual. Defendr runs on a server that intercepts the packages after they have left the third party’s client , but before they reach the application.

## Installation

# Getting started

# Using the System

## Sign in window

This is the first window that the client will see. The client has to enter a username and password, which will then be checked against a Mongo database by retrieving the salted and hashed password for the specific username. If the user’s login was successful they will proceed to the home window of Defendr. The user will be able to close the application by clicking on the close button.

## Home window

This is the main hub of the application, from here a user can navigate to the IP list window, logs window, matrix window or they will have the option to Log out.

## IP list window

This window enables the user to see blacklisted IP addresses and add or remove blacklisted IP addresses from the list. It achieved these functions by using three different queries to the database, namely find, insert and delete respectively.

## Log window

This window enables the user to see either all the packets that went through the system or packets for specific IP addresses. This is achieved through two queries to the database, namely find (to show all packets) and query (to find packets for a specific IP address).

# Troubleshooting