#### SRS Document

**Software Requirements**

**Specifications**

**For**

**VISTA (Visual Intrusion**

**Surveillance and Threat Analysis)**

**Version 1.0**

**Prepared by Aayush Wanem Limbu**

**Itahari International College**

**2025-01-04**

Purpose

The purpose of this Software Requirements Specification (SRS) document is to outline the detailed requirements for the final year project named VISTA () which is a rule based Network Intrusion Detection System (NIDS) project. This document will serve as a guideline for the development, testing and deployment of the system that will ensure that all stakeholders have a clear understanding of the system's functionality, performance, and constraints.

Scope

The NIDS project aims to develop a rule-based intrusion detection system that monitors network traffic, detects known threats using predefined rules, and provides a user-friendly web dashboard for real-time monitoring and management. The system will offer capabilities such as real-time packet capture, alert generation, customizable rule management, and detailed reporting. The primary users of the system will be network administrators responsible for maintaining network security.

**Definitions, Acronyms, and Abbreviations**

NIDS: Network Intrusion Detection System

PCAP: Packet Capture

DoS: Denial of Service

UI/UX: User Interface/User Experience

SRS: Software Requirements Specification

DPI: Deep Packet Inspection

Overall Description

1. Product Perspective

The NIDS will be a standalone system integrating with existing network infrastructures. It will leverage open-source libraries such as Snort for rule-based detection and Django for the web dashboard. The system will be designed to handle high volumes of network traffic efficiently and provide scalability for future expansions.

2. Product Functions

Real-Time Packet Capture & Inspection: Capture and analyze live network traffic to detect suspicious activities.

Alert Generation: Notify administrators of detected threats with categorized severity levels.

Rule Management: Allow administrators to add, update, and delete detection rules.

Report Generation: Provide detailed analysis reports on network traffic and detected threats.

PCAP File Analysis: Enable historical traffic analysis through uploaded PCAP files.

3. User Classes and Characteristics

Network Administrators: Primary users responsible for configuring rules, monitoring alerts, and analyzing reports.

IT Security Teams: Users involved in investigating and mitigating security incidents.

4. Operating Environment

The NIDS will be deployed on a Linux-based server with the following specifications:

OS: Ubuntu 20.04 or later

Processor: Intel i5 11th Gen or equivalent

RAM: Minimum 8 GB (16 GB recommended)

Storage: Minimum 256 GB SSD

2.5 Design and Implementation Constraints

The system must use Python 3.11 or later and Django framework.

The web dashboard must be accessible via modern web browsers (Chrome, Firefox, Edge).

The system should support integration with MySQL for database operations.