# Propose and Scope

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.

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.

Project Goal

1. Rule-Based Detection: Design a NIDS using a rule-based approach (like Snort) to identify threats such as DoS attacks, malware, and unauthorized access.
2. Real-Time Monitoring: Implement real-time traffic monitoring using libraries like Scapy for packet capture and analysis.
3. Customizable Rule Engine: Create a flexible rule engine for admins to adjust and update detection rules based on their network needs.
4. PCAP File Analysis: Allow uploading and analysis of PCAP files for retrospective threat detection.
5. Alerting and Reporting: Develop an alerting system that categorizes threats by severity and provides actionable insights.
6. Network Visualization: Implement network topology visualizations on the dashboard to track and identify unusual devices or activities.
7. Scalability: Optimize performance for high traffic volumes and ensure scalability for larger networks.
8. Web Dashboard: Build an intuitive, web-based dashboard using Django to display real-time traffic stats, alerts, and insights.
9. Real-Time Packet Capture: Continuously capture and analyze packets for detecting suspicious activity.
10. Rule-Based Detection Integration: Match network traffic against predefined signatures to detect known threats.
11. Customizable Rules: Allow admins to easily modify detection rules for specific or emerging threats.
12. Alerting System: Design an alert system with severity categorization (critical, high, medium, low) for prioritized response.

Project Scope

Threat Detection

A rule-based NIDS detects known attacks by comparing network traffic to a list of patterns. If it finds a match, it sends an alert.

2. Real-Time Monitoring and Analysis

The system watches network traffic in real time to spot threats and take quick action. Packet Capture and Analysis tools capture and analyze packets for attack patterns.

3. Customizable Detection Rules

Admins can create, change, or delete rules to address specific threats and network needs, making the system adaptable. The NIDS supports rules ranging from simple packet matches to complex patterns like abnormal network behavior.

4. Alerting and Reporting

The system triggers alerts when it finds traffic matching a known threat, with severity levels. It creates reports with threat details.

5. Retrospective Threat Detection (PCAP File Analysis)

The system can analyze PCAP files to find past threats, useful for forensic investigations. Admins can upload network traffic files for analysis, improving visibility into past security incidents.

6. Scalability and Performance Optimization

The NIDS can manage high traffic volumes without affecting performance, scaling for different network sizes. It optimizes system resources to run efficiently in large, complex networks.

7. Visualization of Network Topology.

The NIDS visualizes the network topology, helping admins spot unusual devices or behaviors for easier detection of unauthorized access. The visualization updates live, giving admins an up-to-date view of the network’s status.

8. User Interface and Usability

Web-Based Dashboard: A user-friendly web dashboard allows administrators to monitor network traffic, view alerts, and analyze reports in real time. Interactive Interface: The dashboard should be intuitive, with interactive components such as drill-down capabilities, customizable views, and quick access to crucial data.

9. Network Security Enhancement

Proactive Defense: By detecting threats early, the rule-based NIDS allows organizations to take proactive measures against potential security breaches. Continuous Monitoring: Ongoing monitoring and quick response to alerts help minimize the impact of cyberattacks.

10. Integration and Compatibility

System Integration: The NIDS should be able to integrate with other security systems (e.g., firewalls, SIEM tools) to provide a more comprehensive security solution. Cross-Platform Support: The system should be compatible with various network environments, such as different operating systems, hardware setups, and network architectures.