Flow Guard

Software Requirements Specification

Version: Beta Version
Status: Under Development

Prepared by CYBER WIZARDS

Date: 14th December, 2024.

Table of Contents

1. Introduction

1.1 Purpose

This Software Requirements Specification (SRS) document provides a detailed description of the software requirements for FlowGuard—a packet inspection and security solution designed to secure network traffic. FlowGuard aims to protect systems from network-based threats by inspecting, filtering, and blocking suspicious or malicious packets. This SRS defines the functional and non-functional requirements, system interfaces, user roles, and external dependencies for the system.

1.2 Scope

FlowGuard is a security tool designed to detect and mitigate threats in real-time by analyzing network packets. The system will analyze data packets in a network, inspect them for potential threats, and prevent malicious data from compromising the network. FlowGuard will provide an interface for administrators to monitor, configure, and manage network security.

This software will be primarily used in enterprise environments to safeguard sensitive data and ensure the reliability of network communications. It supports protocols like TCP/IP, UDP, and ICMP and is intended to be integrated into an existing network security stack.

ID	Stakeholder	Description
S-1	Individual	Used for Benchmarking, Network security
S-2	Student	Used for research purpose, Educational purpose
S-3	IT professional	While developing their website they can use this model for monitoring of their website
S-4	Company	Used for Benchmarking their website servers
S-5	Researcher	Used for research purpose

1.3 Definitions, Acronyms, and Abbreviations

- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System
- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol
- ICMP: Internet Control Message Protocol
- API: Application Programming Interface

1.4 References

- OWASP: Open Web Application Security Project
- RFC 791: Internet Protocol (IPv4)
- RFC 793: Transmission Control Protocol (TCP)
- RFC 9411: Benchmarking Methodology for Network Security Device Performance

1.5 Overview

This document covers:

- Overview of the product and its features
- Functional and non-functional requirements
- System interfaces and architecture
- User roles and interaction with the system
- Detailed analysis of specific features

2. Overall Description

2.1 Product Perspective

FlowGuard is an integrated security solution designed to work at the network layer, inspecting and filtering packets traveling through the system. The product interacts with network adapters, firewalls, and other security infrastructure to analyze, detect, and mitigate security risks in real time. FlowGuard integrates with existing network infrastructures and provides customizable security protocols to suit different environments.

The system is independent of the operating system, designed to run on Linux-based environments, with potential compatibility for Windows-based configurations in future releases.

2.2 Product Features

- Real-Time Packet Inspection: Analyzes incoming and outgoing network packets for suspicious content, malware, or malicious activities.
- Anomaly Detection: Detects deviations from standard network behavior, identifying potential threats such as DDoS attacks, port scanning, or malware communication.
- Customizable Rules: Administrators can define security rules, filters, and thresholds for packet inspection, such as blocking specific IP addresses or filtering certain types of packets.
- Logging & Alerts: Generates logs of network traffic and provides real-time alerts for suspicious activity.
- Network Protocol Support: Supports multiple network protocols including TCP/IP, UDP, and ICMP for diverse network configurations.

2.3 User Classes and Characteristics

- Network Administrators: Configure and monitor security policies, set up alerts, and manage packet filtering rules.
- Security Analysts: Analyze logs, review alerts, and investigate potential network breaches or incidents.
- System Engineers: Perform software installation, integration, and hardware setup for optimal performance of FlowGuard.
- End Users: While FlowGuard is primarily focused on network security personnel, end users might interact indirectly with the system when it blocks or flags their network traffic.

2.4 Operating Environment

- Hardware Requirements:
    - CPU: 2.5 GHz Dual-Core processor (minimum)
    - RAM: 4GB (minimum)
    - Storage: 500GB HDD/SSD
    - Network Interface Cards (NIC): Ethernet, Wi-Fi

- Software Requirements:
    - Linux-based Operating System (Ubuntu, CentOS, or similar)
    - Python 3.x
    - MySQL or PostgreSQL (for logging)
    - Firewall and IDS/IPS Integration

2.5 Constraints

- The system must be capable of running with minimal overhead, using less than 10% of CPU power on average during traffic analysis.
- The system may experience latency with high-volume packet traffic. It should process up to 1,000 packets per second under normal operation.
- FlowGuard should be compatible with IPv4 and IPv6 traffic but will require additional configurations for full IPv6 support.

2.6 Assumptions and Dependencies

- The system assumes that network traffic to be analyzed is already passing through a dedicated network appliance or server where FlowGuard is deployed.
- FlowGuard depends on existing firewall and IDS/IPS systems for additional network protection layers.
- The system requires administrative privileges to configure network filtering rules and other configurations.
-

3. System Features

3.1 Real-Time Packet Inspection

- Description: FlowGuard will inspect every incoming and outgoing packet on the network in real-time. The system will check for signs of malicious content, such as known attack patterns, IP spoofing, or unauthorized protocols.
- Functional Requirements:
    - The system must be able to detect and inspect all IP packets.
    - The system should handle both UDP and TCP packets and ensure no packet bypasses the security inspection.
    - Packet filtering rules should be customizable based on network segments or protocols.
- Use Case:
    - *Title*: Inspecting Incoming Packets
    - *Actors*: Network Administrator
    - *Preconditions*: FlowGuard is running and configured to inspect packets.
    - *Postconditions*: Any packet flagged as suspicious is either blocked or logged for review.

3.2 Anomaly Detection

- Description: FlowGuard will detect unusual network activity that may signify an attack or breach, such as traffic spikes, non-standard ports, or protocol violations.
- Functional Requirements:
    - The system must continuously analyze network traffic against predefined baseline patterns.
    - Alerts must be generated whenever suspicious traffic patterns are detected.
- Use Case:
    - *Title*: Alert on Suspicious Traffic
    - *Actors*: Network Administrator
    - *Preconditions*: FlowGuard is actively monitoring network traffic.
    - *Postconditions*: Alerts are sent to the admin when traffic exceeds baseline thresholds.

3.3 Logging & Alerts

- Description: The system generates logs of network events and sends real-time alerts when specific threats are detected.
- Functional Requirements:
    - Logs should contain detailed information on the packet type, source, and analysis result.
    - Alerts should be configurable to notify administrators via email, SMS, or through an integrated security dashboard.

4. External Interface Requirements

4.1 User Interfaces

- FlowGuard provides a web-based GUI for configuring packet inspection rules, viewing logs, and managing alerts. It should allow real-time monitoring and historical data analysis.

The interface should display:

  - A dashboard with an overview of network traffic
  - Logs of suspicious activities
  - Alerts in real-time

4.2 Hardware Interfaces

- Network Interface Card (NIC): FlowGuard needs to access raw network data via an Ethernet NIC. The software should support various interfaces for different hardware setups.

4.3 Software Interfaces

- Integration with third-party IDS/IPS systems for more advanced threat detection.
- Support for RESTful APIs to enable communication with other network security tools or monitoring systems.

-

5. System Attributes

5.1 Performance Requirements

- FlowGuard should be able to handle a minimum of 1,000 packets per second on a standard 1Gbps network without significant performance degradation.

5.2 Security Requirements

- FlowGuard must enforce secure communication using encryption (e.g., TLS for GUI access).
- The system must log all configuration changes and security events for auditing purposes.

6. Other Non-Functional Requirements

6.1 Scalability

- The system should be able to scale across multiple servers to accommodate large enterprise networks with high traffic volumes.

6.2 Usability

- The user interface should be simple and intuitive for administrators to configure, monitor, and manage security policies.

7. Appendices

7.1 Glossary

- Malware: Software designed to disrupt, damage, or gain unauthorized access to computer systems.
- Packet Filtering: The process of controlling network traffic by monitoring and restricting incoming or outgoing packets.

7.2 Acronyms

- IDS: Intrusion Detection System
- IPS: Intrusion Prevention System

Conclusion

The Software Requirements Specification (SRS) for Flow-Guard - Securing Every Packet outlines a comprehensive framework to ensure the security, reliability, and efficiency of packet transmission in modern network environments. This document defines the system's goals, functional and non-functional requirements, and architectural design, serving as a foundational guide for stakeholders involved in its development and deployment.

By adhering to this SRS, Flow-Guard aims to provide robust packet security mechanisms, including real-time monitoring, encryption, and intrusion prevention, to protect against emerging cyber threats. The clearly defined requirements ensure alignment with industry standards and facilitate seamless integration into existing network infrastructures.

Ultimately, Flow-Guard’s success will depend on rigorous implementation, thorough testing, and ongoing updates to adapt to evolving security challenges. This SRS serves as a blueprint for achieving the project's objectives, delivering a secure, scalable, and user-friendly solution that enhances the integrity of network communication.