# VulZero

Certainly! The requirements for a firewall, IDS, and IPS software with a graphical user interface can be categorized into several key areas. Keep in mind that these are general requirements, and the specific features may vary based on your project goals. Here's an overview:

1. **User Interface:**
   * **Dashboard:** A graphical representation of the network status, current threats, and system health.
   * **Rule Management:** An intuitive interface for defining and managing firewall rules and intrusion detection/prevention rules.
   * **Log Viewer:** A tool to view and analyze logs of network activities and detected threats.
   * **Alerts:** Real-time alerts for suspicious activities or potential security threats.
2. **Network Traffic Handling:**
   * **Packet Inspection:** Capability to inspect incoming and outgoing packets for protocol compliance and anomalies.
   * **Stateful Inspection:** Keep track of the state of active connections and make decisions based on the context of the traffic.
3. **Firewall Functionality:**
   * **Packet Filtering:** Ability to allow or block traffic based on defined rules.
   * **NAT (Network Address Translation):** Support for translating private IP addresses to a public address for outgoing traffic.
   * **Port Forwarding:** Configuration options for directing incoming traffic to specific internal servers.
4. **Intrusion Detection System (IDS):**
   * **Signature-Based Detection:** Identify known patterns of attacks through predefined signatures.
   * **Anomaly-Based Detection:** Detect unusual patterns in network traffic that may indicate a potential threat.
   * **Real-Time Monitoring:** Continuous monitoring of network activities for suspicious behavior.
5. **Intrusion Prevention System (IPS):**
   * **Automated Response:** Ability to take automated actions to prevent or mitigate detected threats.
   * **Traffic Blocking:** Capability to block or limit traffic from sources exhibiting malicious behavior.
6. **Logging and Reporting:**
   * **Event Logging:** Comprehensive logging of security events and activities.
   * **Reporting Tools:** Generate reports summarizing security incidents, network usage, and system health.
7. **User Management:**
   * **Authentication:** Secure mechanisms for user authentication and access control.
   * **User Roles:** Define different roles with varying levels of access to the software.
8. **Updates and Threat Intelligence:**
   * **Update Mechanism:** Regular updates to keep the software current with the latest security patches and features.
   * **Threat Intelligence Integration:** Utilize external threat intelligence feeds to enhance detection capabilities.
9. **Performance and Scalability:**
   * **Performance Optimization:** Efficiently handle network traffic without significant impact on system performance.
   * **Scalability:** Support for larger networks and increasing traffic loads.
10. **Legal and Compliance:**
    * **Compliance Features:** Ensure compliance with relevant laws and regulations.
    * **Audit Trails:** Maintain audit trails to track changes and activities for compliance purposes.
11. **Documentation:**
    * **User Manuals:** Provide comprehensive user manuals and documentation for administrators.
    * **Developer Documentation:** Internal documentation for maintenance and future development.

These requirements provide a foundation for developing a robust firewall, IDS, and IPS software. Depending on your specific use case and target audience, you may need to adjust or expand these requirements.