Team Name - SecureNet Innovators
Team Members - Nabhonil Bhattacharjee, Sampurna Pyne, Dr. Raja Karmakar

Problem Statement: Intrusion Detection/Prevention System (IDS/IPS) Throughput and Latency Benchmarking.

Problem Statement Description: IDS/IPS devices are used to detect and prevent security threats, but their performance can vary with traffic volume, packet sizes, and the complexity of signatures used.

Project Objective: Develop a benchmarking solution to evaluate the throughput and latency performance of an IDS/IPS device/solution.

The solution should support:
→ Different traffic profiles (e.g., regular traffic vs. attack traffic).
→ Signature complexity impact.
→ Latency and packet drop measurements during high-traffic loads.

Deliverables: A tool that benchmarks IDS/IPS devices based on throughput, latency, and detection accuracy under various conditions. The tool should visualize performance degradation as traffic increases.

[RFC 9411]

"Benchmarking Methodology for Network Security Device Performance".
(Published: March 2023)

The solution proposed in reference RFC:

Benchmarking Methodology: The benchmarking tests measure key performance indicators such as throughput, latency, and detection accuracy under controlled conditions.
Traffic Generation Profiles: The RFC emphasizes using varied traffic profiles, including regular (benign) and attack (malicious) traffic, to simulate real-world environments. These profiles include different packet sizes, traffic rates, and protocols to ensure a comprehensive assessment of device capabilities.

Signature Complexity Impact: RFC 9411 recommends using signatures with varying levels of complexity, as IDS/IPS performance can vary significantly based on signature structure and computational load.
Latency and Packet Drop Measurements: The RFC specifies methods for measuring both latency and packet drop rates under increasing traffic loads. The RFC provides a framework for understanding performance degradation and pinpointing bottlenecks by assessing how latency changes as traffic volume grows.
Throughput and Detection Accuracy: A primary focus is on measuring throughput—the maximum rate at which the IDS/IPS can process traffic without significant packet loss or latency—and detection accuracy, which includes the rate of true positives and false positives.

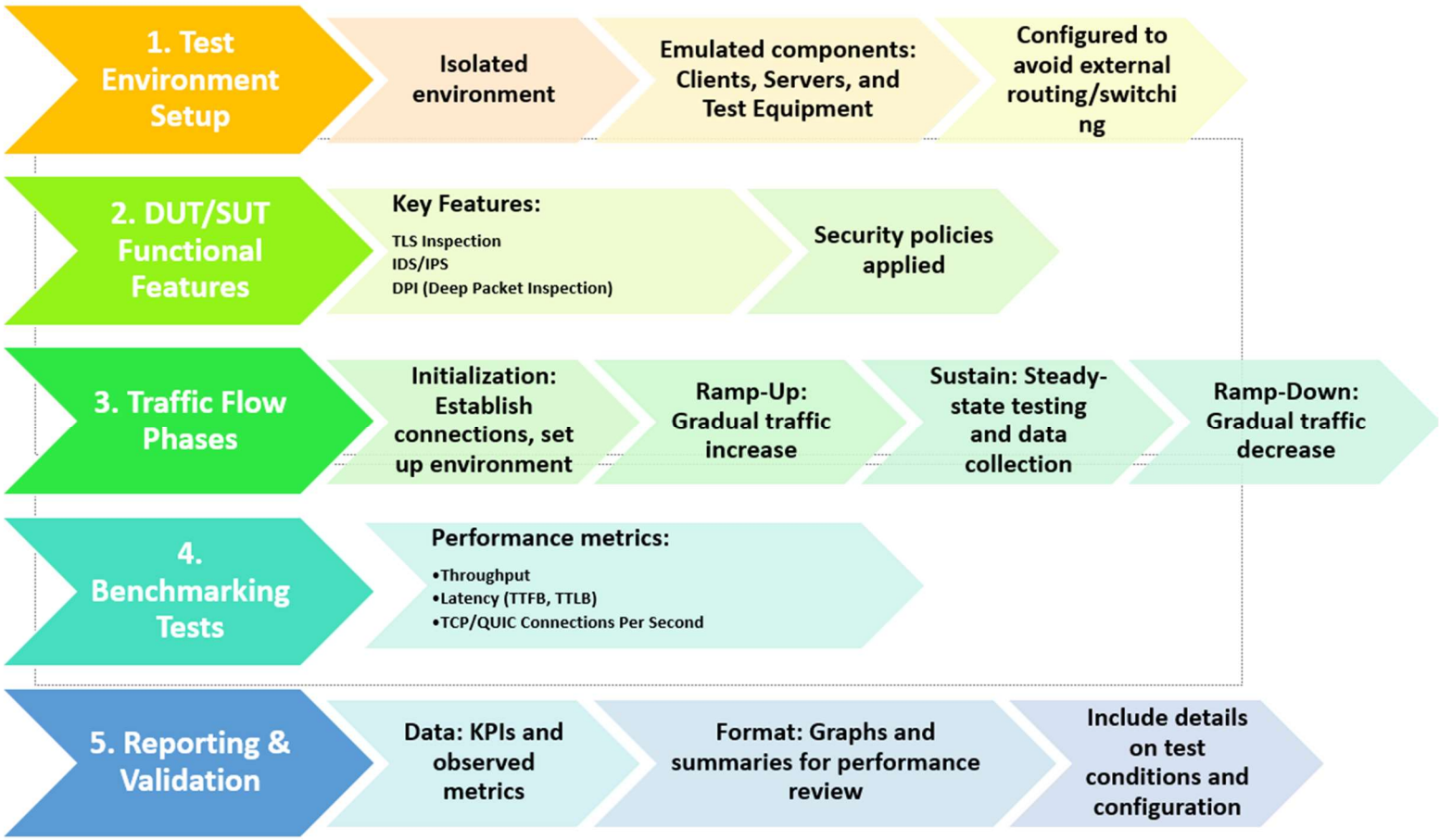
Optimization proposed by our team:

Adaptive Traffic Scaling: Implement dynamic traffic adjustment to simulate sudden load spikes, enabling real-time stress testing of IDS/IPS scalability limits.
Machine Learning Analysis: Use machine learning to analyze performance data, predicting potential failure points and optimizing IDS/IPS configurations for improved resilience.
Visualization Enhancements: Add interactive, real-time visualizations for throughput, latency, and accuracy metrics, offering deeper insights into IDS/IPS performance under varying conditions.

Timeline of Delivery: 2nd December, 2024.

References:
RFC 9411 - Benchmarking Methodology for Network Security Device Performance
Information on RFC 9411 » RFC Editor
Benchmarking Network Security Device Performance with Open Standards - Spirent

WORK FLOW DESIGN:



SOLUTION ARCHITECTURE DESIGN: