Benchmarking Methodology for Source Address Validation

draft-chen-bmwg-savnet-sav-benchmarking-00

Li Chen, Dan Li*, **Libin Liu**, Lancheng Qin

Zhongguancun Laboratory and *Tsinghua University

Outline

- Background
- Motivation
- Goal and Scope
- Test Methodology
- SAV Performance Indicators
- Benchmarking Tests
  - SAV Accuracy
  - Control Plane Performance
  - Data Plane Performance
- Security Considerations

Background: Source Address Validation

- Attacks based on **source IP address spoofing**, such as reflective DDoS and flooding attacks, continue to present significant challenges to Internet security.
- Mitigating these attacks in intra-domain and inter-domain networks requires effective source address validation (SAV).
- BCP84 proposes some intra-domain and inter-domain SAV solutions, such as ACL-based ingress filtering and uRPF-based SAV mechanisms, and operators are suggested to deploy different SAV mechanisms [RFC3704] [RFC8704] based on their deployment network scenarios.
- Intra-domain and inter-domain SAVNET mechanisms are proposed in SAVNET WG to solve existing SAV mechanisms' problems in validation accuracy and operational overhead.
  - https://datatracker.ietf.org/doc/draft-ietf-savnet-intra-domain-architecture/
  - https://datatracker.ietf.org/doc/draft-wu-savnet-inter-domain-architecture/

Motivation

- Proposing standard benchmarking methodology is important for evaluating the performance of intra-domain and inter-domain SAV mechanisms fairly
  - For network operators, the benchmarking methodology can help them get a more accurate idea about the performance of the SAV devices in their deployed network environments, in order to utilize the appropriate SAV mechanism.
  - For device vendors, the benchmarking methodology can help vendors test the performance of the SAV implementation for their devices.
  - The benchmarking methodology can guide how to evaluate whether the new intra-domain SAV mechanisms can satisfy the design requirements defined in [draft-ietf-savnet-intra-domain-problem-statement] and the new inter-domain SAV mechanisms can satisfy the design requirements defined in [draft-ietf-savnet-inter-domain-problem-statement].

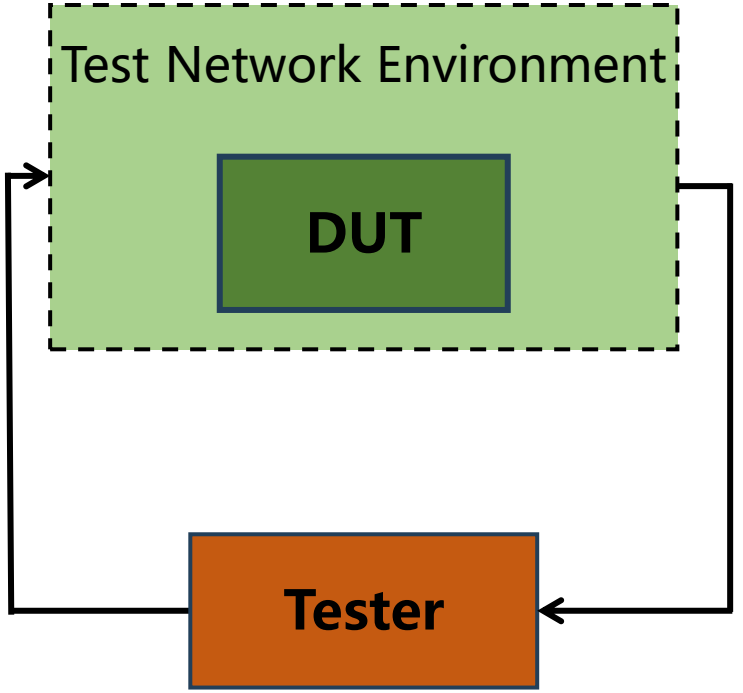
Goal and Scope

- **Two objectives** of the benchmarking methodology:
  - Assessing "which SAV mechanisms perform best" over a set of well-defined scenarios.
  - Measuring the contribution of sub-systems to the overall SAV systems' performance (also known as "micro-benchmark").
- SAV device under test (**DUT**)
  - The benchmark aims to test the performance of individual SAV devices, e.g., hardware or software routers.
  - The benchmark will showcase the performance of various SAV mechanisms for a given SAV DUT and network scenario, with the objective of deploying the appropriate SAV mechanism in the corresponding scenarios.

Test Methodology

Test Setup

- Test network topology: The DUT is connected to other network devices to construct the network topology.
  - The location where the DUT resides in the network topology affects the accuracy of SAV mechanisms.
- Tester
  - The Tester can be connected to the DUT directly or by other devices.
  - The Tester can generate traffic to test the accuracy, control plane performance, and data plane performance of DUT.
  - The network traffic generated by Tester should specify traffic rate, the proportion of spoofing and legitimate traffic, and the distribution of source addresses.
- DUT role and device configurations
  - The DUT role, such as host-facing router, customer-facing router, and AS border router in the intra-domain network, and the business relationship between ASes in the inter-domain network, is related to the SAV accuracy.
  - The device in the network topology can have various routing configurations and the generated SAV rules of DUT is also determined by the configurations of other devices.



Test Setup

SAV Performance Indicators

- Proportion of Improper Blocks
  - The proportion of legitimate traffic which is blocked improperly by the DUT across all the legitimate traffic, and this can reflect the SAV accuracy of the DUT.
- Proportion of Improper Permits
  - The proportion of spoofing traffic which is permitted improperly by the DUT across all the spoofing traffic, and this can reflect the SAV accuracy of the DUT.
- Protocol Convergence Time
  - The protocol convergence time represents the period during which the SAV control plane protocol converges to update the SAV rules, and it is the time elapsed from the beginning to the completion of the SAV rule update. This can indicate the SAV control plane performance of the DUT.

SAV Performance Indicators

Protocol-speaking Agent Processing Throughput

- The protocol-speaking agent processing throughput measures the throughput of processing the packets for communicating SAV-related information on the control plane, and it can indicate the SAV control plane performance of the DUT.

Data Plane SAV Table Refreshing Rate

- The data plane SAV table refreshing rate refers to the rate at which a DUT updates its SAV table with new SAV rules, and it can reflect the SAV data plane performance of the DUT.

Data Plane Forwarding Rate

- The data plane forwarding rate refers to the SAV data plane forwarding throughput for processing the data plane traffic, and it can reflect the SAV data plane performance of the DUT.

Benchmarking Tests

Intra-domain and Inter-domain SAV

- SAV accuracy: proportion of improper blocks and proportion of improper permits.
- Control plane performance
  - Protocol convergence performance: protocol convergence time.
  - Protocol-speaking agent performance: protocol-speaking agent processing throughput.
- Data plane performance
  - Data plane SAV table refreshing performance: data plane SAV table refreshing rate.
  - Data plane forwarding performance: data plane forwarding rate.

SAV Accuracy of Intra-domain and Inter-domain SAV

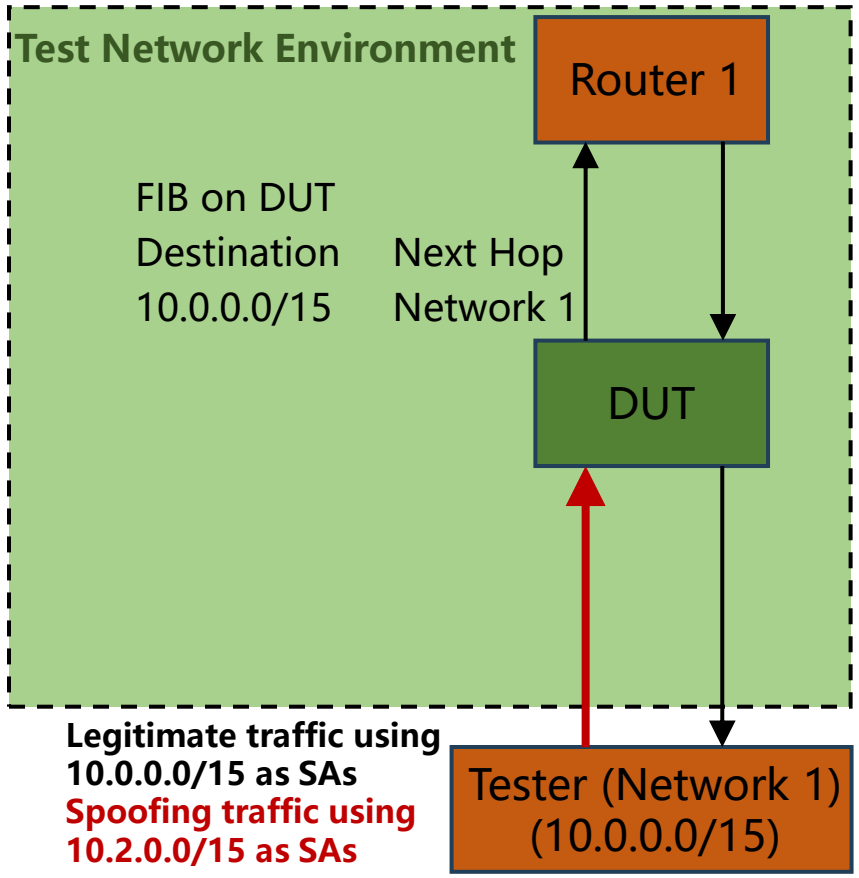
Objective

- Measure the SAV accuracy of the DUT to process legitimate traffic and spoofing traffic in various intra-domain network scenarios including SAV for customer or host Network, SAV for Internet-facing network, and SAV for aggregation-router-facing network, and in various inter-domain network scenarios including SAV for customer-facing ASes and SAV for provider/peer-facing ASes.

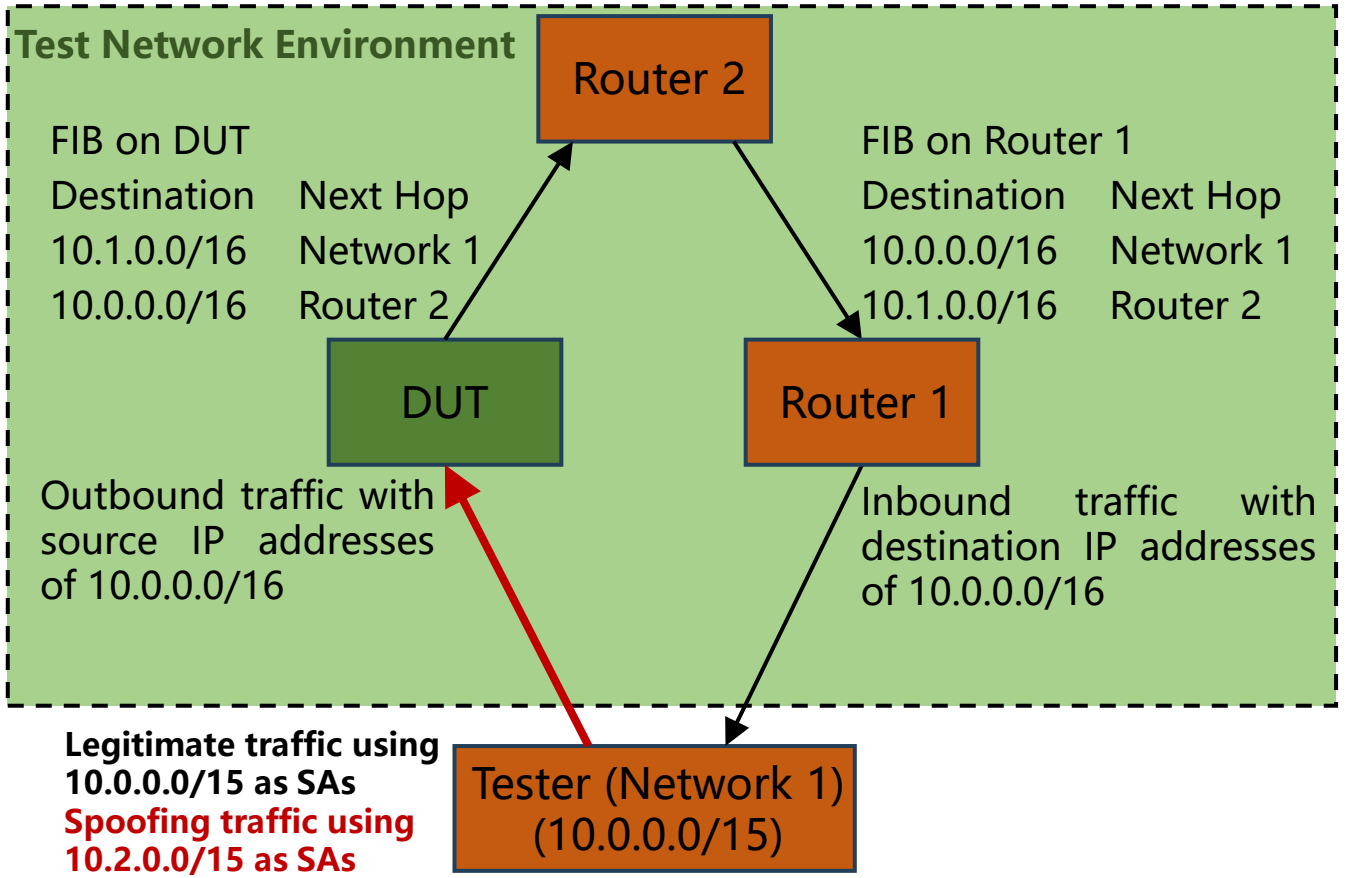
Test Scenarios

- Intra-domain SAV
  - SAV for customer or host network
  - SAV for Internet-facing network
  - SAV for aggregation-router-facing network
- Inter-domain SAV
  - SAV for customer-facing ASes
  - SAV for provider/peer-facing ASes

Intra-domain SAV: SAV for Customer or Host Network



(a) Test Case 1: SAV for customer or host network in intra-domain symmetric routing scenario.



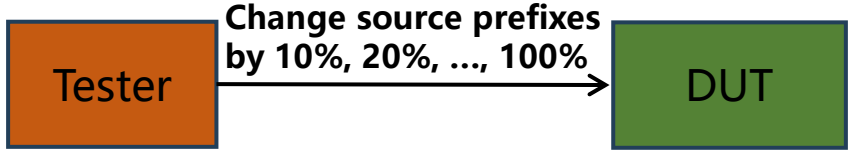
(b) Test Case 2: SAV for customer or host network in intra-domain asymmetric routing scenario.

- **Expected Results**: The DUT can permit the legitimate traffic (e.g., SAs in 10.0.0.0/15) and block the spoofing traffic (SAs in 10.2.0.0/15) from Network 1 for the above test cases.

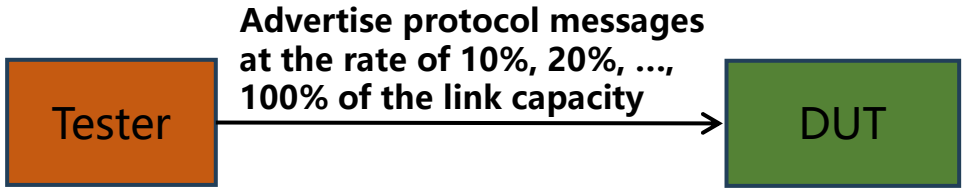
Control Plane Performance of Intra-domain and Inter-domain SAV

Objective

- Measure the protocol convergence performance of the DUT and the protocol-speaking agent performance for processing protocol packets.



(a) Protocol convergence performance test



(b) Protocol-speaking agent performance test

Protocol convergence performance

- Protocol convergence time is calculated by subtracting the beginning time from the completion time of the protocol convergence process.

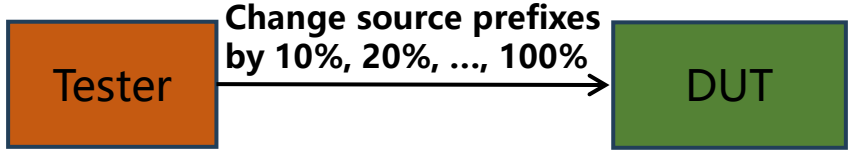
Protocol-speaking agent performance

- Protocol-speaking agent processing throughput is calculated by dividing the overall size of the protocol messages by the overall processing time.

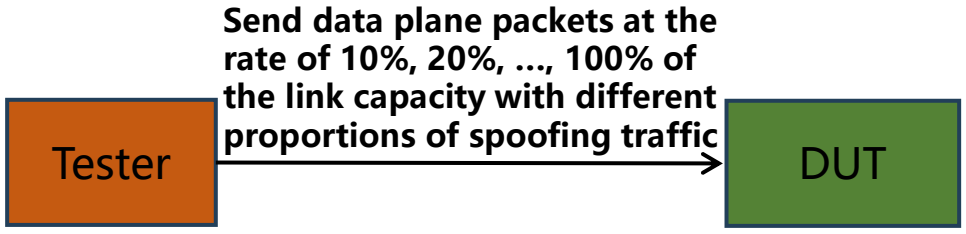
Data Plane Performance of Intra-domain and Inter-domain SAV

Objective

- Measure the data plane SAV table refreshing performance of the DUT and the data plane forwarding performance for forwarding data plane packets.



(a) Data plane SAV table refreshing performance test



(b) Data plane forwarding performance test

Data plane SAV table refreshing performance

- Data plane SAV table refreshing rate is calculated by dividing the overall number of the updated SAV table entries by the overall SAV table refreshing time.

Data plane forwarding performance

- Data plane forwarding rate is calculated by dividing the overall size of the data plane packets by the overall forwarding time without packet drop.

Security Considerations

- Test the DUT in a laboratory environment
  - The benchmarking tests described in this document are limited to the performance characterization of SAV devices in a lab environment.
- Isolated from the production network
  - The benchmarking testbed will be an independent one and MUST NOT be connected to devices that may forward the test traffic into a production network.

Next Step

- Seek feedback and comments.
- Collaborations are welcome.

Thanks! ☺