SHENICK SOLUTION BRIEF

Testing Packet Inspection Appliances with TeraVM

OVERVIEW

TeraVM is used to assess the performance and functionality of packet inspection and policy enforcement appliances. TeraVM that ensures each and every flow is correctly identified and/or policed according to the configured policy settings.

FEATURES

- ✓ Emulate traffic up to 1 Terabit per second (Tbps)
- ✓ Stateful emulation with L2-7 parameter configuration
- ✓ Packet replay with amplification for non-native application types
- ✓ Per flow performance measurements, with problem flow notification. Pre-configured tests for throughput and latency testing at scale
- ✓ Concurrent testing with IPv4 and IPv6 application flows and mixed frame sizes
- ✓ Automated traffic profiling with randomness
- ✓ Dynamic control: bring endpoints or applications in/out of service during live test runs

SHENICK

www.shenick.com

Packet inspection and policy enforcement appliances play a key role in modern networking with a wide range of uses such as network traffic analysis, media management (in LTE networks), optimization of traffic flows and to detect security threats.

A critical challenge for packet inspection is the ability to correctly identify every traffic signature at wire speed with zero impact on the integrity of the data. In addition, when a policy is applied to the traffic flow it must not adversely impact performance.

TeraVM is the only IP test solution available which can perform per flow analysis, thereby simplifying the challenge of understanding if the packet inspection appliance is properly identifying each and every traffic flow's characteristics. More importantly, TeraVM provides a comprehensive set of performance measurements on each and every emulated traffic flow. TeraVM is used to automatically notify the user of any traffic flow which has been impacted by poor policing policies. Even after generating hundreds of millions of unique flows, isolating the problem has never been simpler.

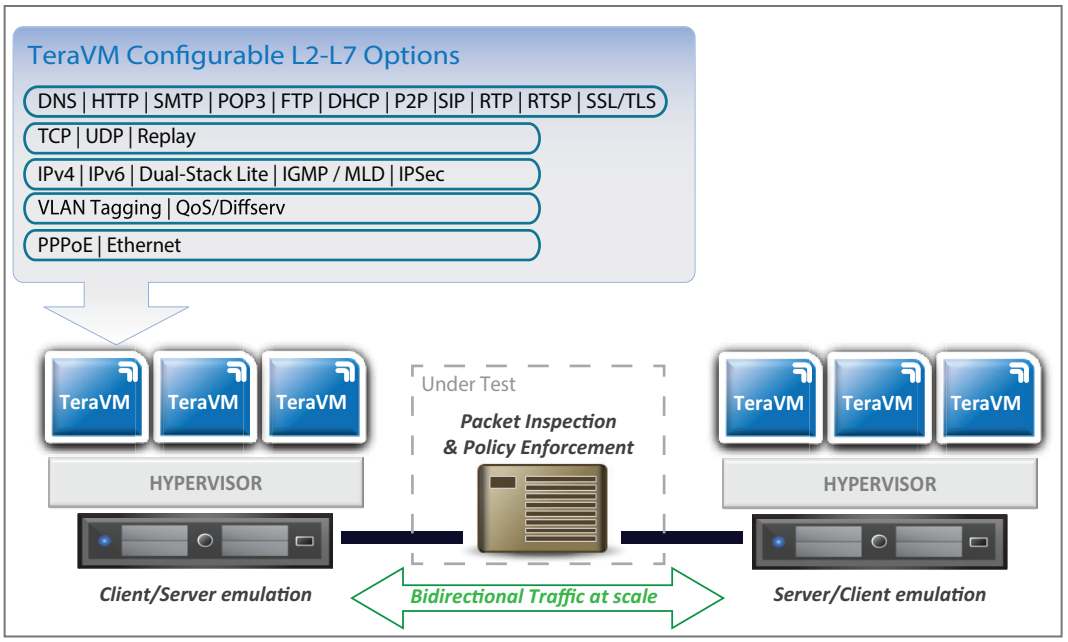

Figure 1: Example TeraVM deployment

Packet Replay

TeraVM provides emulation of many of the leading application types, for non-native applications TeraVM uses packet replay. TeraVM's packet replay benefits customers because it allows them to continually test with the latest application signatures. Furthermore, TeraVM supports amplification of packet captures allowing the customer to model future usage profiles. These two key steps are fundamental in determining if the packet inspection appliance is accurately identifying the latest applications and is correctly graphing usage profiles.

TeraVM's replay functionality supports:

- ✓ Raw Port Playback (whole capture file replay, configure start/stop details)
- ✓ TCP Replay (emulate client/server, optional use of original timestamps, replay multiple files)
- ✓ UDP Replay (includes stateless protocol flow replay)

Testing Packet Inspection Appliances with TeraVM

Comprehensive Test Capability

TeraVM provides the industry's most comprehensive test suite with over 3,000 unique metrics; ranging from application performance to protocol tunneling down to simple port enabled testing with throughput and latency metrics. A user defined threshold can be set on any of these metrics to easily pinpoint and isolate problem flows.

TeraVM provides detailed analysis on each and every emulated flow, the following highlighting some of those key metrics:

- ✓ Packets per second
- ✓ Dropped/Out of Sequence Packets
- ✓ Retransmitted Packets
- ✓ Jitter
- ✓ Latency
- ✓ TCP Connection Rate
- ✓ Application Goodput
- ✓ Unique Application timings
- ✓ Video/ Audio quality score

Functionality Overview

Use Case	Description
Needle in the IP Stack	- Emulate tens of millions of subscribers, with hundreds of millions of flows. - Emulate a single subscriber with illicit content, identify if the emulated subscriber is identified and the policy enforcement is correctly deployed.
False Positive/False Negative ID	- Ensure that all emulated flows are classified correctly with minimum handling errors. - Test that no flow is misclassified (e.g. a mix up between corporate email and web based email).
User and Usage profiling	- Emulate a profile of mixed traffic, emulate multiple application flows per endpoint. - Dynamically bring endpoints in/out of service to vary profile patterns, determine if pattern matches what is being recorded by the inspection appliance. - Test with the latest traffic signatures, use packet replay to add the latest device and application traffic types.

TeraVM Software Overview

GENERAL
- Real-time isolation of problem flows

DATA
- TCP / UDP
- HTTP (headers, substitution, attachments)
- SMTP / POP3 (incl. file attachments)
- FTP (Passive/Active)
- P2P applications
- DNS

ADDRESS
- MAC, VxLAN
- DHCP, PPPoE (IPv4 & IPv6)
- Dual Stack (6RD, DS Lite)

ETHERNET SWITCH
- VLAN & Double Tagging (Q-Q)
- ACL, 802.1p, DSCP

REPLAY
- Replay large PCAP files
- Amplify and dynamically substitute data into PCAP files
- TCP, UDP and raw data playback

VIDEO
- Multicast: IGMP v1/v2/v3 & MLD v1/v2
- Automatic Multicast Tunelling (AMT)
- Video on Demand (VoD)
- Adaptive Bit Rate Video (HLS, HDS, Smooth)
- Video conferencing

SECURE VPN
- SSL/TLS/DTLS
- IPsec (IKE v1/v2)
- Cisco AnyConnect SSL VPN Client
- Cisco AnyConnect IPsec VPN Client
- 802.1x EAP-MD5

SECURITY ATTACK MITIGATION
- Spam / Viruses / DDOS

VOICE
- VoIP: SIP & RTP (secure & unsecure)
- Dual Hosted UACs, SIP Trunking
- H.323
- Voice & Video quality metric (MOS)

LTE/4G
- GTP tunnel support

SLA
- TWAMP

AUTOMATION
- CLI, Perl, TCL, XML, Java API

SHENICK

NORTH AMERICA
1900 McCarthy Blvd, Suite 301
Milpitas, CA 95035, USA
TEL: 408-385-7630

EUROPE
Brook House, Corrig Avenue,
Dun Laoghaire, Dublin, Ireland
TEL: +353-1-236-7002

www.shenick.com
info@shenick.com

id: 060613