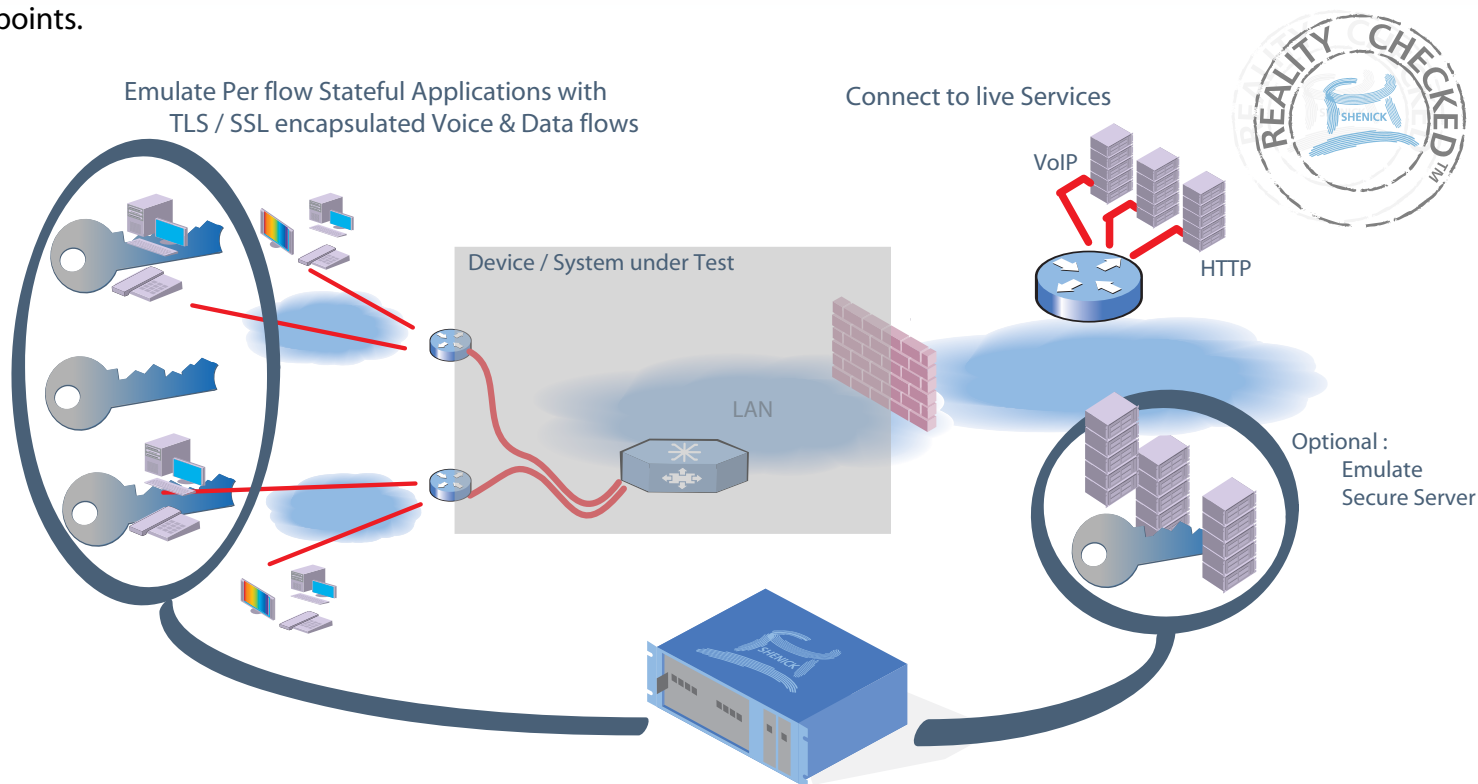




# Testing with TLS/SSL diversifEye™ Flows

TLS / SSL secures communication through the encryption of the application traffic flows in IP networks, which improves the end-user QoE by mitigating against stolen information. The most widely used and important revenue generating applications to which TLS / SSL provides security include voice and data.

diversifEye uses TLS / SSL to enable the most realistic flow functionality required to test components such as Call Managers, Firewalls, IMS SBCs, etc. diversifEye's emulated end points go through the key phases such as negotiation of algorithms, exchange of keys, authentication and cipher/decipher of traffic flows transmitted between emulated end points.



## Sample Scenario tests with TLS / SSL diversifEye flows

### TLS / SSL End Point Performance -

Emulate on a 'Per flow' end point basis individual traffic flows. Determine performance of non encapsulated flows versus encapsulated TLS / SSL flows across system under test.

### Secure Voice Bulk Calling -

Benchmark network devices such as SBCs or firewalls, through performance measurements of large volumes of emulated TLS / SSL encapsulated SIP flows. Determine QoE on a per flow, per individual end point basis. Examine individual call performance and voice quality.

### Mixed traffic flow Performance -

Emulate and analyze the effect of large volumes of TLS / SSL flows when combined with other non encrypted applications such as IPTV, VoD, P2P, etc. Examine performance when bad or 'illegal' flows are added to the mix which may include DDoS / Viruses / Worms / Spam.



diversifEye 'Per flow' architecture enables users to configure not just one but thousands of TLS/SSL individual unique sessions, each supporting multiple applications.

diversifEye as an integrated solution provides performance measurements for each and every session and/or application running in real time.

diversifEye™ is the only integrated network, application and security attack emulation and performance analysis IP test system providing granularity on a per flow basis for emulated end points with secure encrypted flows with TLS / SSL.

diversifEye's per flow architecture provides unrivaled control on a per flow basis for volume or load testing. diversifEye's traffic profiling may include a mix of TLS / SSL encrypted and non encrypted application flows.

The Shenick diversifEye platform and GUI supports per flow test and measurement of :

### Analysis Software Overview

- DHCPv4 & DHCPv6
- PPPoE
- VLAN & Double Tagging (Q-in-Q) with priority
- Concurrent IPv4 and IPv6 application flows
- IGMP V1, V2, V3, MLD V1, V2
- Voice and Video Quality Metrics  
(both no reference and full reference analysis)
- RTSP (Video on Demand)
- VoIP (SIP & RTP)
- HTTP
- FTP
- SMTP
- POP3
- P2P
- TWAMP
- Attack Traffic - Spam / Viruses / DDOS
- PCAP file replay (>1Gb)

### Why use diversifEye's TLS / SSL solutions

- Real Voice and Data      diversifEye's TLS / SSL flows use real voice and data when emulating end points. Measure performance or voice quality using no reference analysis and MOS scores.
- Stateful Protocol Flows      Emulate stateful IP flows for unique end points and applications. By using stateful / real TCP flows it's possible to see how the individual TLS / SSL end points handle congestion.
- Quality of Experience      Ensure in real-time, on a per flow TLS / SSL basis that the network or device settings have no impact on the encrypted voice application, especially under varying QoS settings.
- Security Attack Mitigation      It is equally important to measure performance under extreme conditions. The TLS /SSL connections must remain open while unwanted traffic such as spam or even DDoS attacks are happening in the network.

### diversifEye Summary Features and Benefits

- Network QoS and per flow QoE granularity for individual emulated client users across multiple devices and application traffic flow types.
- Latest protocols supported from Data Applications (HTTP, FTP, POP/SMTP, P2P), IPTV (IGMP/MLD), VoD (RTSP), VoIP (SIP/RTP) all in a single test package.
- TCP Replay Substitution, automatically varies payloads so no two PCAP sessions are the same.
- Support for TWAMP, IPv4 and IPv6.
- DHCP emulation, PPPoE and IPoE Service Interoperability Scenarios. Emulate per device MAC and IP address assignments.
- Security Attack Mitigation support for DDoS style attacks SYN/RST/UDP/ARP floods, reflective DDoS attacks, Ping of death, etc.
- Large memory space (>1Gb) for PCAP replay for Instant Messaging or Web Mail.
- Client and server support on a single blade within one chassis with complete flexibility on port allocation. Full support for multiple daisy chained chassis all controlled from a single GUI.
- Low cost of ownership and ease of use by avoiding multiple test systems and non integrated software applications.

diversifEye™ is a trademark of Shenick Network Systems. All other trademarks are the trademarks of their respective owners.

North America | 533 Airport Boulevard, Burlingame, CA 94010, USA      Tel: +1-650-288 0511      Fax: +1-650-745 2641  
 Europe | Brook House, Corrig Avenue, Dun Laoghaire, Dublin, Ireland      Tel: +353-1-236 7002      Fax: +353-1-236 7020

web: [www.shenick.com](http://www.shenick.com)      email: [info@shenick.com](mailto:info@shenick.com)

© 2010, Shenick Network Systems Limited

(Shenick Version No. - v3.0)