



# **diversifEye™** **Field Application Notes**

Testing with TLS/SSL secure  
media flows in diversifEye

**Shenick Network Systems**



# **diversifEye™**

Per flow Converged IP Network Test Systems



## ***Table of Contents***

INTRODUCING 'PER FLOW' .....	4
A CLOSER LOOK AT SECURE VOIP FLOW PROCESSING.....	5
THE VALUE OF STATEFUL END POINT EMULATION.....	6
'PER FLOW' PERFORMANCE MEASUREMENTS .....	7
FURTHER 'PER FLOW' PERFORMANCE TESTS.....	8
SUMMARY OF 'PER FLOW' PERFORMANCE TESTS WITH TLS/SSL SECURE MEDIA.....	9

## Overview

The following application note outlines some of the necessary test requirements for testing the performance of secure media flows with real applications such as voice, video and data. The objective of the application note is to correlate how the various components such as firewalls, registration servers and call management servers impact quality performance of the application within the secure flows.

- For secure voice flows, performance is assessed on a per individual voice call basis with an emphasis on measuring voice quality with Mean Opinion Scores (MoS).
- For secure video flows, performance is assessed on a per individual video flow basis with an emphasis on measuring video and audio quality through MoS.
- For secure data applications, performance is assessed on an individual end point's connection rate performance and an emphasis on latency performance measurements.

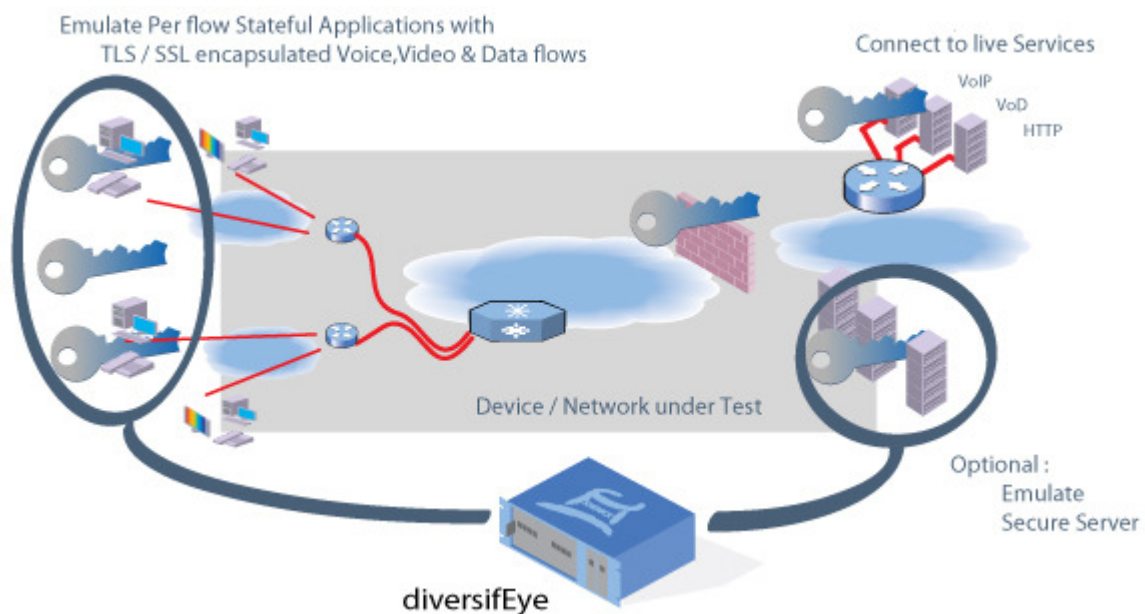


Figure 1 - Example walled environment with secure flows, diversifEye emulating both end point and servers

## Introducing 'Per flow'

'Per flow' network and application emulation and analysis, delivers real world proof of concept, demonstration and testing for secure media and walled environments. Per flow testing is further enhanced by the ability to emulate actual deployments of several thousand individual end points running many different application types, over common services such as DHCP / PPPoE / VLAN and TLS/SSL as necessary.

A single configurable unique flow -

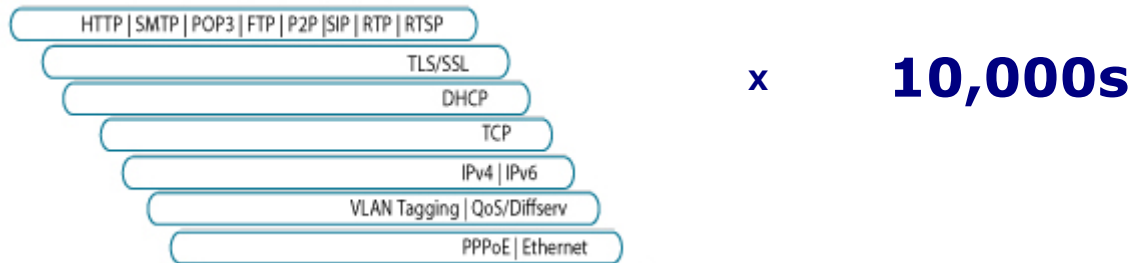


Figure 2 - Configurable flows for thousands of end points

When it comes to reviewing performance of the device or system under live test conditions, 'Per flow' provides the necessary granularity to view each of the individual uniquely emulated end points performance. That is, from the tens of thousands of emulated end points, it's possible to select one end point and view the individual application performance in terms of activity and transmitted media flow quality e.g. (VoIP calling attempt activity performance and Voice quality MoS / R-factor).

Is there a benefit to 'Per Flow' granularity for secure media testing?

**Secure Voice flows:** A sample test scenario for testing with 'Per flow' for call managers includes testing configurations such as maximum seat numbers, establish the knock on effects when the maximum number of call users are connected and an extra end point attempts registration. For firewalls, a sample 'Per flow' test is emulating peak hour conditions, determine root cause and affect on quality when integrating different call origin devices or codecs.

**Secure Video flows:** In a similar manner for secure video flows, measure performance in terms of the number of concurrent sessions capable on secure servers. Negative test with corrupt digital certificates, examine the impact on video performance or MoS scores when both legal and illegal flows present.

**Secure Data flows:** 'Per flow' testing is not limited by the application types or per end point, a sample test scenario is to emulate bad/illegal flows, vary testing by including bogus account users, examine performance of individual end points when a DDoS type attack occurs on data servers.

**Be real, test with mixed traffic flows!**

With 'Per flow' the possibility for varying traffic scenarios are endless, in almost a similar manner to real networking environments it's possible to find any multiples of applications including the nasty: Virus, Worms and Spam. Even behind walled environments or with secure media flows there is always the possibility of interference to quality from illegal traffic flows.

## ***A closer look at secure VoIP flow processing***

QoE is seen as a summation of performance of an integrated number of events. Essentially a voice call is a chain of events, in which each event or chain link is as strong as the last. Therefore, it's important to analyze the process for quality and performance from start to finish.

On further breakdown, it's possible to see that on each of the individual integrated links a number of a failure points exist and overall performance and quality may be impacted –

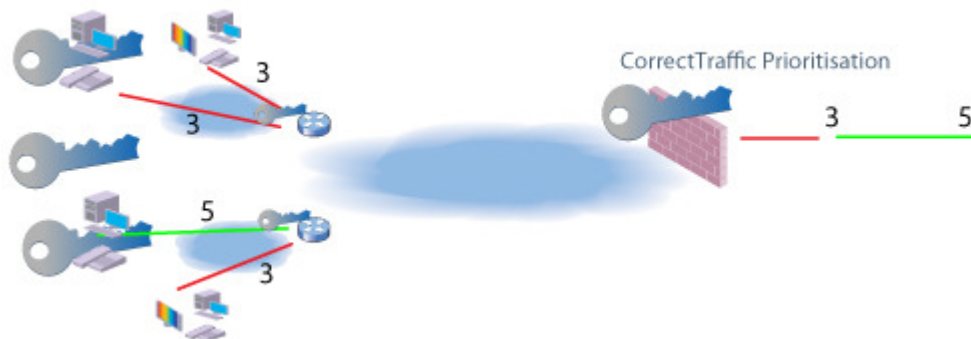
What are the potential failure points or poor QoE in a secure VoIP call?

- Configuration of the End point – how fast can the TFTP file be accessed and downloaded?
- Provisioning the End point – IP address assignment, how fast can the DHCP server respond?
- Registration of the End point – how quick is the SIP proxy/registration authentication?
- Inbound / Outbound Connectivity – Is the SIP proxy server routing configuration correct?
- Network Overload – What impacts have retransmits for SIP requests on the call manager?
- Media Encryption – Can calls be sustained with encrypted media flows (SRTP)?
- Call Media Quality – How much latency can an end point tolerate?

This is one unique flow, is it possible to emulate several thousand of these flow processes?

The above is a sample of just one end point media session, in real world terms the process occurs over thousands of unique end points. Therefore testing needs to be scalable, not forgetting that communication is a two way flow, with various handshaking and negotiations e.g. (SIP Invite/Bye, TCP window resizes, etc).

Performance testing with secure media and walled environments requires end points to be stateful. This is extremely useful in examining the impact of rate limiting of a firewall. A sample test scenario for heavy traffic flows is to check that the correct priorities are being managed, so that out of thousands of flows, each flow with its varying Diffserv / CoS is handled correctly by the firewall.



*Figure 3 - Stateful flows with TCP window negotiation, Diffserv / CoS priorities*

## **The value of stateful End Point Emulation**

An important aspect in performance testing with secure flows is the ability of the endpoint to connect to the relevant secure location such as the call manager or the ability to pass flows through firewalls. This means that each end point must be in a position to exchange digital certificates, negotiate ciphers and recognise keys.

*NOTE : In emulating the characteristic of any IP based device such as IP Phones a certain amount of bespoke configuration is required, in this case the IP phone must interoperate with firewalls, TLS proxies, phone proxies, etc. It's clearly of benefit at an early stage to choose a test and measurement solution that offers this flexibility.*

### **Is there a tangible benefit to a stateful end point address negotiation in performance testing?**

It's important to include the major components that may impact performance or overall quality of the flows. For example, when IP address allocation is through PPPoE, DHCPv4/v6 servers then the performance of these servers need to be assessed. The ability of an end point to register for an IP address and how quickly it receives an IP address is a fundamental part of the overall QoE for a service.

A sample set of tests may include:

- Concurrent Requests – Max number of MAC addresses register/deregister per second.
- Authentication Performance – AAA service latency performance.
- Throughput Requests – Max number of sessions sustainable per second.

When it comes to going live, having tested with stateful end points with secure media, ensures when the real devices such as a VoIP phone attempts to register it will do so first time.

### **What configuration or performance issues may occur during/after securing the communication with TLS?**

Voice end point configuration performance: Once the end point is assigned an IP address, the next step for the secure calling end point is to set up its local configuration usually through the use of XML or TFTP.

Video end point configuration performance: In a similar manner an emulated secure video device may download an electronic program guide before it connects through to a default video source/channel.

Therefore performance testing should include some of the following scenario measurements:

- Access File server - Max number of concurrent end points connecting per second.
- File Download Performance – Bandwidth / Latency performance.
- Busy Hour Attempts – Max connections during periods of heavy congestion.

## 'Per flow' Performance measurements

### Unleashing the Power of 'Per flow'

End points exchange media flows over a mix of both RTP and SRTP, in large scale numbers. Large volumes of end points may be ramped up in blocks, whilst benchmarking the performance of the system under test, the call manager, firewall etc.

Once the end points establish a session it's possible to measure on each and every end point the application performance in real time.

A sample of the 'Per flow' metrics that offer the most information in terms of quality for voice, video and data (http) are listed below (for more information on the performance metrics or for other applications, email [info@shenick.com](mailto:info@shenick.com)) -

VoIP Emulated End Point & Application Performance	Video Emulated Application Performance	HTTP Emulated Application Performance
UA In RTP Bits/sec	QmVideo Picture Quality	Client Out Bits/s
UA Out RTP Bits/sec	QmVideo MOS	Client Out Packets/s
UA In RTP Packets/sec	QmVideo Transmission Quality	Client Out of Sequence In Packets
UA Out RTP Packets/sec	QmVideo Multimedia MOS	Client Retransmitted Packets
UA RTP Out of Sequence Packets	QmVideo Mean PDV (Average Packet Delay Variation)	Client Attempted Connections/s
UA RTP Dropped Packets	QmVideo Max PDV (Maximum Packet Delay Variation)	Client Established TCP Connections/s
UA Duplicate RTP Packets	QmVideo Stream ID	Client Failed TCP Connections/s
UA Out Calls Attempted	QmVideo Codec	Client 200 Responses/s
UA Out Calls Established	QmVideo In Packets	Client 100-199/201-299 Responses/s
UA Out Calls Rejected	QmVideo Out Of Sequence Packets	Client 300-399 responses/s
UA In Calls Attempted	QmVideo Dropped Packets	Client 400-499 Responses/s
UA In Calls Established	QmVideo Discarded Packets	Client Other Responses/s
UA In Calls Rejected	QmVideo Underrun Discarded Packets	SYN/SYNACK Count
UA Calls Errored	QmVideo Overrun Discarded Packets	SYN/SYNACK Mean ms
UA SIP Out Messages	QmVideo Duplicate Packets	SYN/SYNACK Min ms
UA SIP Messages Resent	QmVideo In I-Frames	SYN/SYNACK Max ms
UA SIP In Messages	QmVideo Impaired I-Frames	SYN/Data Count
UA In RTCP Packets	QmVideo In P-Frames	SYN/Data Mean ms
UA Out RTCP Packets	QmVideo Impaired P-Frames	SYN/Data Min ms
UA Registrations Attempted	QmVideo In B-Frames	SYN/Data Max ms
UA Registrations Successful	QmVideo Impaired B-Frames	FIN/FINACK Count
UA Registrations Rejected	QmVideo Frames/s	FIN/FINACK Mean ms
UA Registrations Errored	QmVideo Frame Width	FIN/FINACK Min ms
UA Calls Received Ringing	QmVideo Frame Height	FIN/FINACK Max ms
UA Mean Time to Ringing (ms)	QmVideo GoP Length	
UA Min Time to Ringing (ms)	QmVideo GoP Type	
UA Max Time to Ringing (ms)	QmMp2ts TS_sync_loss	
UA Calls Received RTP Packet	QmMp2ts Sync_byte_error	
UA Mean Time to RTP Packet (ms)	QmMp2ts Continuity_count_error	
UA Min Time to RTP Packet (ms)	QmMp2ts Transport_error	
UA Max Time to RTP Packet (ms)	QmMp2ts PCR_repetition_error	
UA RTP Jitter (RFC 3350) ms	QmMp2ts PCR_discontinuity_indicator_error	
UA RTP Max Jitter (RFC 3350) ms	QmMp2ts PTS_error	
QmVoice MOS		
QmVoice RFactor		
QmVoice Stream ID		
QmVoice Codec		
QmVoice In Packets		
QmVoice Dropped Packets		
QmVoice Out Of Sequence Packets		
QmVoice Duplicate Packets		
QmVoice Discarded Packets		
QmVoice Underrun Discarded Packets		
QmVoice Overrun Discarded Packets		
QmVoice Mean PDV ms (Packet Delay Variation)		
QmVoice Max PDV ms (Packet Delay Variation)		

Table 1 - Sample Voice, Video, data layer 7 metrics

**NOTE :** In 'Per flow' testing, emulated end points may have multiple applications running e.g. emulate a PC with voice, video, data. Therefore, each end point may have multiple performance statistics. All these application performance measurements make up the QoE at that end point.

## Further 'Per flow' Performance Tests

### TLS / SSL Performance measurements of Firewalls, Call managers, etc

Traffic flows traversing the firewalls, call managers, IMS SBCs should experience minimum disruption in terms of quality and performance issues. The various management devices should not add unnecessary latency to the TLS/SSL enabled flows.

A sample set of test scenarios includes:

- Mixed traffic flows – Performance of encrypted and non-encrypted media streams (SRTP / RTP)
- Latency of SRTP flows – Establish if the firewall impedes SRTP based flows, assess the voice quality in open media sessions.
- Max Throughput – Number of sessions possible across firewalls and call managers.

### TLS / SSL performance between trusted and untrusted end points

The end point is considered to be a trusted device once its registers correctly with the various management functions. Following this the end points are used to establish sessions with other end points, in which the end points will pass media over both RTP and SRTP.

A sample set of test scenarios includes:

- Trusted to Trusted – Establish calls between end points in walled environment.
- Trusted to Untrusted – Establish calls outside walled environment.
- Untrusted to Untrusted – Establish calls in walled environment with unknown end points.

### TLS / SSL Security Performance

By using 'Per flow' test and performance measurements, Service Providers and Network Equipment Vendors, may test for security breaches, in emulating end points with plain SIP/RTP and secure end points with TLS/SRTP.

It's important to test the integrity of the firewall, call management system with the exchange of invalid digital certificates. In this TLS / SSL security example, a mix of traffic flows are presented with both valid legal and fraudulent illegal certificates.

The ability to add a single illegal/invalid certificate to an emulated end point, captures the essence of 'Per flow', with thousands of flows in session it's now possible to measure the firewall's, call manager's, etc performance in terms of isolating maligned endpoints and invalid certificates.

### Real World Scenario testing, with the good, bad and illegal.

In the real world, networks will have more than just voice or data flows but a mix of genuine and malicious traffic flows containing everything from IPTV streams, VoD requests, web and email downloads to unfavourable bad or illegal traffic flows such as email virus/worm attacks, spam generation, DDoS attacks on servers, etc .

It's also worth considering a mix of traffic with the malicious exploitation of protocols as part of the test strategy, if only to determine the cause and effect on quality of the TLS/SSL encapsulated flows.

## ***Summary of 'Per flow' Performance Tests with TLS/SSL Secure Media***

'Per flow' emulation and performance measurement has simplified and made the testing of management systems, firewalls, call managers, etc, more realistic by emulating as close as possible, the real configuration of the actual end points in use on the network, plus more importantly the activity and applications running on the emulated end points.

When it comes to 'Per flow' performance measurements, the winning feature is the ability to emulate thousands of end points which are configured instantly in a test, and at any stage during the live testing an individual end point may be selected and its details looked at in great depth, in particular the layer 7 application performance. This simple trait of the 'Per flow' architecture provides the granularity required in understanding the difference in application layer quality on TLS / SSL enabled flows.

In walled environments and management of secure media flows, testing secure and unsecure flows alongside each other provides visibility in how the various components such as the firewalls or call managers handle the TLS / SSL enabled flows versus the plain unsecure IP flows.

Service Providers and Network Equipment Vendors can now fine tune their secure communication systems by emulating and analyzing the end point characteristics such as cipher negotiation, key exchange and certificate handling. Another useful 'Per flow' test enables testing of false certificates, extreme conditions or attacks with large volumes of certificate exchange requests.

In real networks there is likely to be more than one traffic type or flow existing. It's paramount when it comes to testing with secure media, that these other flows which may contain illegal traffic such as email viruses and spam, are added to the mix. This becomes essential in testing the security vulnerabilities of firewall devices.

Finally, the most important quality measurement of any environment is defined as the performance of the application, the voice quality, the video quality or the data flow performance. This is a key component of real subscriber QoE measurements, how the end user perceives the voice quality as audible, video as viewable or data access times as tolerable. TLS / SSL enabled flows are not isolated from network problems or issues and the very output of the application media at the end point, must be considered.

'Per flow' testing can determine application quality in terms of MoS / R-factor for secure voice. For secure video, quality is measured in terms of MoS on both the video and audio quality. Finally, for secure data, performance and quality may be measured in terms of connection rates, mean get times, etc.

Take a reality check in testing the performance of your secure environments or secure media flows, try 'Per flow' testing today!

Shenick is an award winning provider of 'Per flow' IP communications test and measurement systems. Shenick's diversifEye and servicEye are used to assess and monitor network, application and security infrastructure performance limitations.

diversifEye™ and servicEye™ are integrated network, application and security attack emulation and performance assurance test systems which are used by major IP-oriented network service providers, communications equipment manufacturers, large enterprises and governments.

Shenick's diversifEye addresses key next-generation converged network and application performance issues covering IPTV, Voice, Data, IMS, Security Attack Mitigation, Traffic Shaping/Peer to Peer (P2P), Application Server, Metro Ethernet and IPv4/IPv6 hybrid network deployments.

Shenick's servicEye is an active multiservice monitoring solution, born out of award winning and industry proven quality assessment technology on an end-to-end basis.

Shenick is the proud recipient of Internet Telephony's 2008 Product of the Year and IPTV Excellence awards. Adding further to these achievements are the Frost and Sullivan 2008 Global Technology Innovation Award for DPI. Other awards from Frost and Sullivan include the 2007 Global Product Innovation Award, 2006 Emerging Company of the Year Award in the Communications Test and Measurement industry sector along with the 2005 European Product Line Strategy Award.

## Shenick Network Systems

**Ireland** : Brook House, Corrig Avenue, Dun Laoghaire, Co Dublin, Ireland

t: +353-1-2367002

[info@shenick.com](mailto:info@shenick.com)  
[sales@shenick.com](mailto:sales@shenick.com)

### Regional Support Email Contact Details -

Americas: [amer-support@shenick.com](mailto:amer-support@shenick.com)

Asia Pacific: [apac-support@shenick.com](mailto:apac-support@shenick.com)

Europe, Middle East & Africa: [emea-support@shenick.com](mailto:emea-support@shenick.com)

## Global Sales & Support

**North America** : 533 Airport Boulevard, Burlingame, CA 94010, USA

t: +1-650-288-0511

**Germany** : Elsterweg 140, D-72793 Pfullingen, Germany

t : +49-7121-383-6882

**Singapore** : 3 Raffles Place, #07-01 Bharat Building, Singapore 04817

t: +65-9788-5945

© 2009 Shenick Network Systems Limited. All rights reserved, subject to change without notice. diversifEye and servicEye are trademarks of Shenick Network Systems, all other names are trademarks of their respective owners and hereby acknowledged.