



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

Testing with TLS/SSL/IPSec  
secure media flows in diversifEye

**Shenick Network Systems**



# **diversifEye™**

Per flow Converged IP Network Test Systems



## ***Table of Contents***

OVERVIEW .....	3
INTRODUCING 'PER FLOW' .....	4
A CLOSER LOOK AT A SECURE ENDPOINT FLOW PROCESSING .....	6
THE VALUE OF STATEFUL ENDPOINT EMULATION .....	7
'PER FLOW' PERFORMANCE MEASUREMENTS .....	8
FURTHER 'PER FLOW' PERFORMANCE TESTS .....	9
SUMMARY OF 'PER FLOW' PERFORMANCE TESTS WITH TLS/SSL/IPSEC.....	10

## 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, Telepresence 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 Telepresence flows, performance is assessed on a per tunnel per individual Telepresence session with unique measurements on both the video and voice quality (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 endpoint's connection rate performance and an emphasis on latency performance measurements.

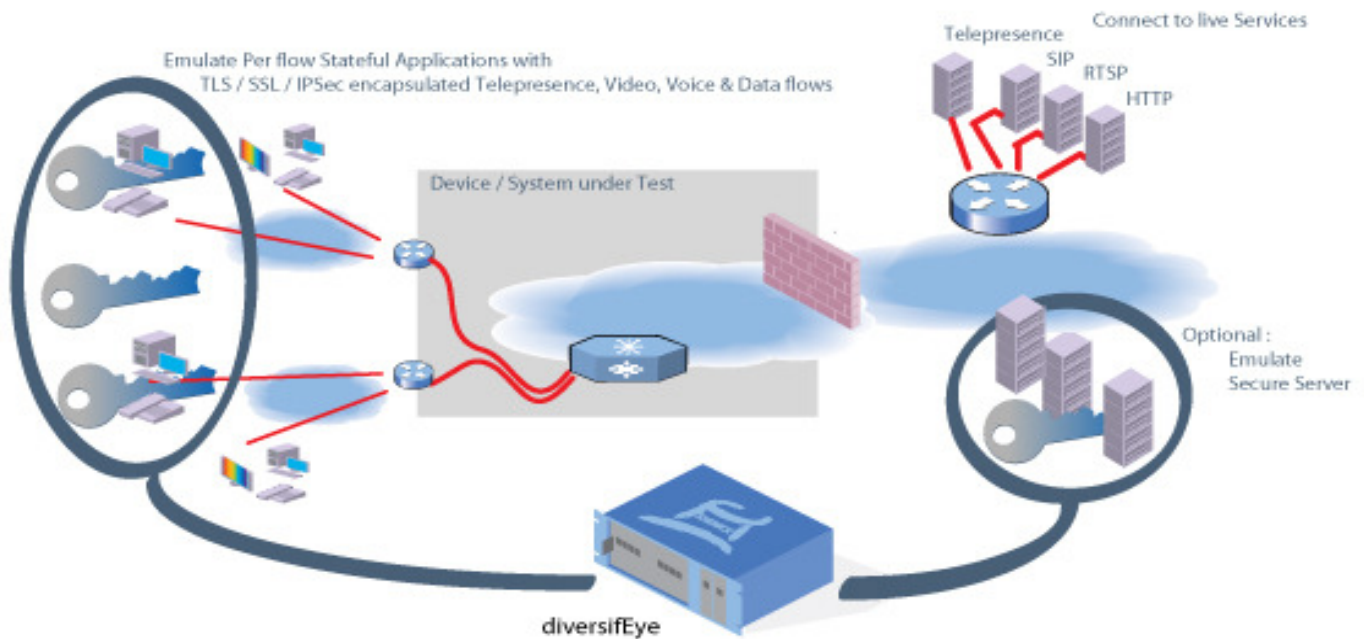


Figure 1 - Example walled environment with secure flows, diversifEye emulating both endpoint and servers

## 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 endpoints running many different application types, over common services such as DHCP / PPPoE / VLAN and TLS / DTLS / SSL / IPSec as necessary.

A single configurable unique flow -

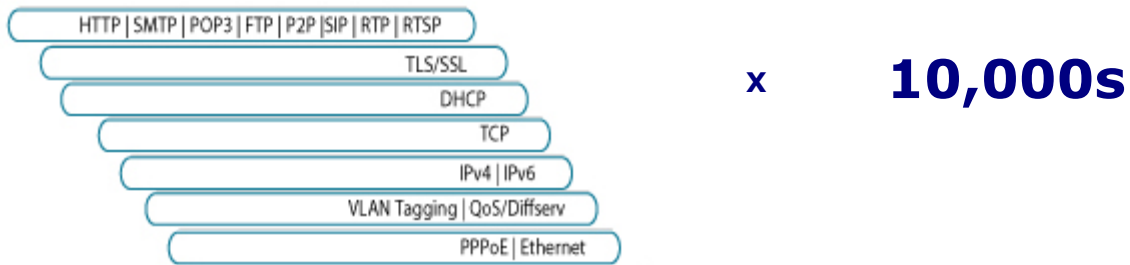


Figure 2 - Configurable flows for thousands of endpoints

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 endpoints performance. That is, from the tens of thousands of emulated endpoints, it's possible to select one endpoint 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 endpoint 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.

**Telepresence flows:** Telepresence is a delay sensitive application. It's important to understand the impact secure tunnelling has on each flow in the Telepresence session. Per flow provides the benefits of measuring on a per tunnel, per Telepresence flow basis. Assess how different policy settings on the endpoint secure server impact each component part of the Telepresence session.

**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 endpoint, a sample test scenario is to emulate bad/illegal flows, vary testing by including bogus account users, examine performance of individual endpoints 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 a secure endpoint flow processing***

QoE is seen as a summation of performance of an integrated number of events. Essentially, a secure voice call or secure Telepresence session are a chain of events inside a tunnel. Therefore, it's important to analyze on an end-to-end basis the quality and performance from initial tunnel request to tunnel teardown.

On further breakdown, it's possible to see that each application in the tunnel has an individual integrated number of steps, all of which may act as QoE failure nodes. Stateful testing isolates issues between tunnel configuration/policies and actual application issues –

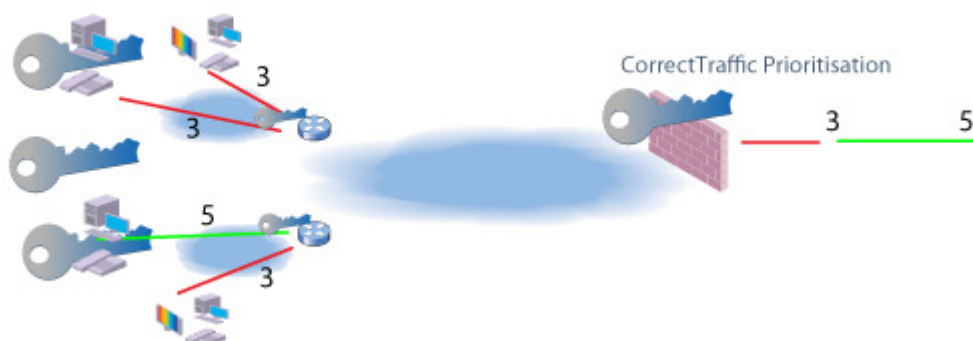
What are the potential failure points or poor QoE in a secure Telepresence or VoIP call, outside of the secure tunnel?

- Configuration of the Endpoint – how fast can the TFTP file be accessed and downloaded?
- Provisioning the Endpoint – IP address assignment, how fast can the DHCP server respond?
- Registration of the Endpoint – 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 endpoint tolerate?

Is it possible to scale to several thousands of test flows?

The above is a sample of just one endpoint media session in a secure mode. 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 endpoints to be stateful. Another use of stateful traffic is the ability to examine the impact of rate limiting of a firewall. A sample test scenario is for periods of heavy traffic flows, all the time checking 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 Endpoint 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 endpoint 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 the Telepresence endpoint or IP Phone requires a certain amount of bespoke configuration. In the case of an IP phone it 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 endpoint address negotiation in performance testing secure tunnels?

It's important to include the major components that may impact performance or overall quality of the application inside the secure tunnel. For example, when IP address allocation is through PPPoE or DHCPv4/v6 servers then the performance of these servers need to be assessed. The ability of an endpoint 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.

What configuration or performance issues may occur during/after securing the application with TLS / DTLS / IPsec?

Voice endpoint configuration performance: Once the endpoint is assigned an IP address, the next step for the secure calling endpoint is to set up its local configuration usually through the use of XML or TFTP. Latency issues may see a device default to an unknown setting.

Video endpoint 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. Again incorrect policy may result in the EPG failing to traverse the SUT.

Rekeying: IPsec rekeying is major part of how the protocol operates. Understanding rekeys is essential in determining the QoE impact on delay sensitive applications like Telepresence meetings.

Performance testing of the applications inside the tunnels should include some of the following scenario measurements:

- Access File server - Max number of concurrent endpoints connecting per second.
- File Download Performance – Bandwidth / Latency performance.
- Busy Hour Attempts – Max connections during periods of heavy congestion.
- Duration testing – determine how rekeys shape performance.

## 'Per flow' Performance measurements

### Unleashing the Power of 'Per flow'

Endpoints exchange media flows over a mix of both protocols, in large scale numbers. Large volumes of endpoints may be ramped up in blocks, whilst benchmarking the performance of the system under test, the call manager, firewall etc. Once the endpoints establish a session it's possible to measure on each and every endpoint 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	Telepresence Client Application Item
UA In RTP Bits/sec	QmVideo Picture Quality	In service
UA Out RTP Bits/sec	QmVideo MOS	Registrations Attempted
UA In RTP Packets/sec	QmVideo Transmission Quality	Registrations Successful
UA Out RTP Packets/sec	QmVideo Multimedia MOS	Registrations Rejected
UA RTP Out of Sequence Packets	QmVideo Mean PDV (Average Packet Delay Variation)	Registrations Errored
UA RTP Dropped Packets	QmVideo Max PDV (Maximum Packet Delay Variation)	Out Calls Attempted/s
UA Duplicate RTP Packets	QmVideo Stream ID	Out Calls Established/s
UA Out Calls Attempted	QmVideo Codec	Out Calls Rejected
UA Out Calls Established	QmVideo In Packets	In Calls Attempted/s
UA Out Calls Rejected	QmVideo Out Of Sequence Packets	In Calls Established/s
UA In Calls Attempted	QmVideo Dropped Packets	In Calls Rejected
UA In Calls Established	QmVideo Discarded Packets	SIP Out Messages
UA In Calls Rejected	QmVideo Underrun Discarded Packets	SIP Messages Resent
UA Calls Errored	QmVideo Overrun Discarded Packets	SIP In Messages
UA SIP Out Messages	QmVideo Duplicate Packets	Calls Errored
UA SIP Messages Resent	QmVideo In I-Frames	In RTCP Packets
UA SIP In Messages	QmVideo Impaired I-Frames	Out RTCP Packets
UA In RTCP Packets	QmVideo In P-Frames	Mean time to RTP packet ms
UA Out RTCP Packets	QmVideo Impaired P-Frames	Max time to RTP packet ms
UA Registrations Attempted	QmVideo In B-Frames	Min time to RTP packet ms
UA Registrations Successful	QmVideo Impaired B-Frames	Calls Received RTP Packet
UA Registrations Rejected	QmVideo Frames/s	Calls Received Ringing
UA Registrations Errored	QmVideo Frame Width	Mean time to Ringing ms
UA Calls Received Ringing	QmVideo Frame Height	Max time to Ringing ms
UA Mean Time to Ringing (ms)	QmVideo GoP Length	Min time to Ringing ms
UA Min Time to Ringing (ms)	QmVideo GoP Type	RTP Video Frame Jitter Max ms
UA Max Time to Ringing (ms)	QmMp2ts TS_sync_loss	RTP Video Frame Jitter Mean ms
UA Calls Received RTP Packet	QmMp2ts Sync_byte_error	RTP Video Frame Count
UA Mean Time to RTP Packet (ms)	QmMp2ts Continuity_count_error	RTP Duplicate Packets
UA Min Time to RTP Packet (ms)	QmMp2ts Transport_error	RTP Dropped Packets
UA Max Time to RTP Packet (ms)	QmMp2ts PCR_repetition_error	RTP Out of Sequence Packets
UA RTP Jitter (RFC 3350) ms	QmMp2ts PCR_discontinuity_indicator_error	RTP Receive SSRC
UA RTP Max Jitter (RFC 3350) ms	QmMp2ts PTS_error	RTP Send SSRC
QmVoice MOS		In RTP Packets/s
QmVoice RFactor		In RTP Bits/s
QmVoice Stream ID		Out RTP Packets/s
QmVoice Codec		Out RTP Bits/s
QmVoice In Packets		QMVideo MOS
QmVoice Dropped Packets		QMAudio MOS
QmVoice Out Of Sequence Packets		QMVideo Underrun Discarded Packets
QmVoice Duplicate Packets		QMVideo Overrun Discarded 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, Telepresence metrics

NOTE: In 'Per flow' testing, emulated endpoints may have multiple applications running inside secure tunnels. Therefore, each secure tunnel has multiple performance statistics. All these application performance measurements make up the QoE at that endpoint.

## Further 'Per flow' Performance Tests

TLS/SSL/IPSec Performance measurements of Secure Gateway Servers, Firewalls, Call managers, etc Traffic flows traversing the secure gateway servers, 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/IPSec 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 Number of secure sessions – Number of concurrent sessions on the securing device.
- Aggregate Application Throughput – Number of applications e.g. Telepresence, data, etc

### TLS / SSL / IPSec performance between trusted and untrusted endpoints

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

A sample set of test scenarios includes:

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

### TLS / SSL / IPSec Security Performance

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

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

The ability to add a single illegal/invalid preshared key to an emulated endpoint, 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 / preshared keys.

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

In the real world, networks will have more than just Telepresence, 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 bad or illegal traffic flows such as email virus/worm attacks, spam generation, DDoS attacks on servers, etc .

It's 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/IPSec**

'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 endpoints in use on the network, plus more importantly the activity and applications running on the emulated endpoints.

When it comes to 'Per flow' in secure mode, a critical feature is the ability to emulate the tunnel configuration process and behind each tunnel add any number of application flows such as Telepresence, Voice, video or data.

The winning benefit for diversifEye is not just the per tunnel configuration performance measurements, but the fact users can measure actual application quality on each and every flow in each and every tunnel. This provides an accurate representation on how policies and settings impact the tunnel item but also the delay sensitive applications such as Telepresence, Voice or Video. This simple trait of the 'Per flow' architecture provides the granularity required in understanding the difference in application layer quality on TLS / SSL / IPSec 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 / IPSec 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 endpoint 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. Its 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 / IPSec enabled flows are not isolated from network problems or issues and the very output of the application media at the endpoint, 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 Network Systems

**North America:** 533 Airport Boulevard, Burlingame, CA 94010, USA  
t: +1-650-288-0511

**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)

© 2010 Shenick Network Systems Limited. All rights reserved, subject to change without notice. The material contained in this document is for general information purposes only and does not constitute technical or professional advice. diversifEye and servicEye are trademarks of Shenick Network Systems, all other names are trademarks of their respective owners and hereby acknowledged.  
Rev: 2v0-2010