

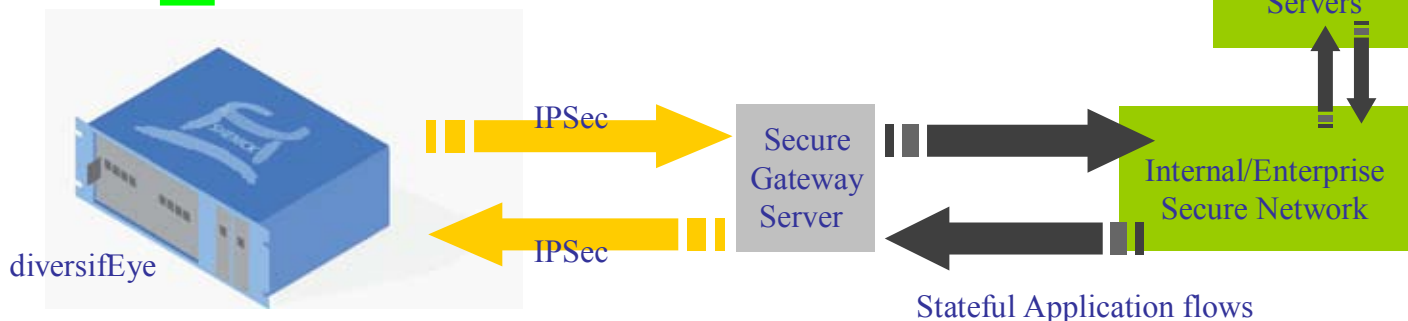
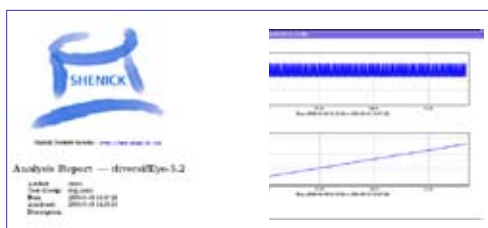
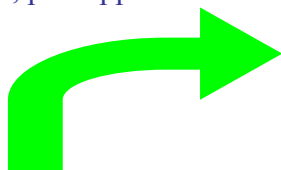


Testing IPsec tunnel and application performance with diversifEye

Defining the correct balance of security policies in IPsec is essential in ensuring network security and the ability to deliver a reasonable level of Quality of Experience for the IPsec tunneled application. Testing secure sever gateway performance is dependent on how the tunnel setup performs plus the ability to deliver real applications such as telepresence, video, voice and data in the configured tunnels.

diversifEye's 'Per flow' architecture enables users configure hundreds of individual unique IPsec tunnels with multiple unique applications and activity per tunnel. The key benefit of testing with diversifEye is the ability to measure performance on each and every IPsec tunnel, but more importantly on each and every application running in the tunnels.

QoE /QoS Performance Measurements:
Per IPsec Tunnel, per Application



Shenick represents the real IPsec Tunnel requesting endpoint, each unique session initiator may negotiate an individual IPsec session, to which real traffic flows are attached. diversifEye supports both IKEv1 and IKEv2 using ESP and AH protocols, over tunnel mode. A wide variety of popular encryption and authentication algorithms are supported. diversifEye's flexibility covers authentication mechanisms through digital certificates and/or pre-shared keys.

Sample test scenarios in which diversifEye's emulated IPsec endpoints are used :

- IPsec VPN Aggregate Throughput
- Per VPN Throughput
- Per Application Throughput e.g. (HTTP, Telepresence, SIP, etc)
- Application quality e.g. (Voice MoS, Video MoS, etc)



IPsec Security Considerations

Like all internet based protocols IPsec is vulnerable to malicious attacks. IKE Denial of Service (DoS) attacks are used to tie up valuable CPU processing cycles, the aim, to stop any new tunnel sessions being connected. Service Providers and Vendors need to test systems for the negative by including a mix of real and attack traffic flows. To generate the right traffic mix a per flow solution such as Shenick's diversifEye is required.

diversifEye IPSec features

- Support IKEv1, IKEv2
- Tunnel Protocol Mode
- Diffie Hellman - 1, 2, 5
- Encryption Algorithms - 3DES, DES, AES-256, AES-192, AES-128
- Support for Phase I and Phase II rekeying
- Authentication Algorithms - SHA-1, MD5
- Authentication Mechanisms - Digital Certificates, Pre-shared Keys
- IPv4-in-IPv4 IPSec Tunnels

Emulate stateful endpoints :

- Unique IPSec tunnels
- Multiple traffic flows per tunnel
- Performance measurements per tunnel, per application



- IPv6-in-IPv4 IPSec Tunnels, (private = v6, public = v4)
- Application Traffic secured by IPSec - Telepresence, Voice (SIP& RTP), Video (RTSP), Data (HTTP, SMTP, POP3)

Connect through 3rd party secure gateway servers to 3rd party application servers

Sample diversifEye test cases

Network Capacity Testing

Examine network capacity with a small number and/or many emulated IPSec endpoints, threshold test acceptable packet loss. Create real world scenarios with mixed application traffic loads (secure and unsecure). Examine the impact on each and every emulated IPSec end-point's application quality.

Security Appliance Testing

Test security appliances such as firewall, Email / web proxies and filters, IPS/IDS with real application flows. Examine each and every emulated end-points application quality under varying network load conditions.

Secure End-Point performance

Establish IPSec sessions with secure gateway servers, send real application requests over the established secure tunnels. diversifEye is used to emulate many individual unique end points and measures in real time per endpoint per application performance.

Cable Infrastructure testing (DOCSIS 3.0)

diversifEye is used to emulate anything from a single flow to several thousand CPEs and flows, functionality includes both CPE and server side application emulation, providing the complete test structure for CMCI to CMTS-NSI. Examine DOCSIS 3.0 CM and CMTS performance under extreme conditions or large volume requests. Analyze application quality on emulated CPEs using IPv6 versus IPv4. Analyze traffic mixes, including dual stack enabled applications.

diversifEye Functionality Overview

- Telepresence (incl. TIP)
- VoIP (SIP & RTP)
- Multicast Video (IGMPv1,2,3 & MLDv1,2)
- VoD (RTSP, SIP enabled RTSP, HTTP enabled RTSP)
- Voice and Video Quality Metrics
- HTTP ver 0.9, 1.0, 1.1 (GET, POST incl. attachments)
- FTP
- SMTP
- POP3
- P2P, P2P replay
- IPSec/TLS/SSL - secure flows
- DHCPv4, DHCPv6, PPPOE
- VLAN & Double Tagging (Q-in-Q) with priority
- Concurrent IPv4 and IPv6 application flows
- Dual-Stack Lite, 6rd
- TWAMP
- Attack Traffic - Spam / Viruses / DDOS
- PCAP file replay (>1Gb)

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

email: info@shenick.com

© 2010, Shenick Network Systems Limited

(Shenick Version No. - v1.0)