Testing Security of IP Networks with diversifEye™

SHENICK

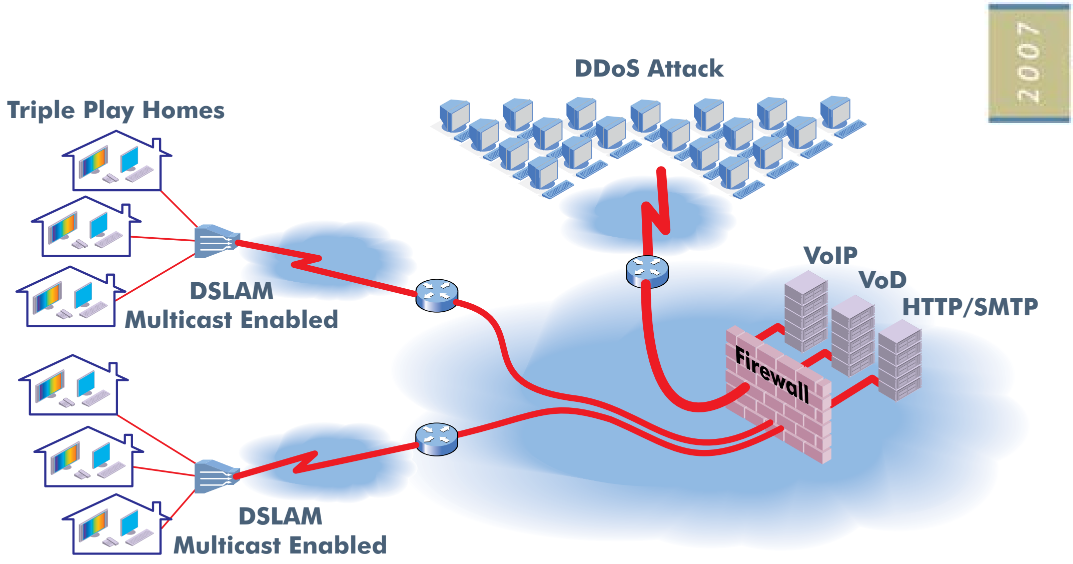
IP networks and protocols are susceptible to security attacks through malicious content such as viruses and worms distributed denial of service (DDoS) attacks as well as the prolifteration of Spam.

Establishing performance limitations for converged IP services such as Triple Play is critical for high quality performance applications such as IP Video/IPTV and VoIP. Another key feature to the converged IP network is the potential traffic load the network will need to handle during busy hours.

In addition to regular load scenarios there is also a growing need to pay attention to sustaining quality of experience issues during security attacks. Networks today must not only mitigate security attacks but also guarantee uninerrupted subscriber experience.

diversifEye™ is the first integrated emulation and performance analysis platform providing complete virtualization of real clients and/or servers and security attack generation. Users may determine network performance in normal or attack conditions by generating traffic loads of genuine user activity or a traffic mix which includes malicious traffic (DoS, Viruses, Worms and Spam). diversifEye™ provides a secure, controlled environment in which tests can be delivered, and performance limitations can be assessed, in real time.

2007 FROST & SULLIVAN Global Product Innovation Award



TOLLY Up to Spec CERTIFIED

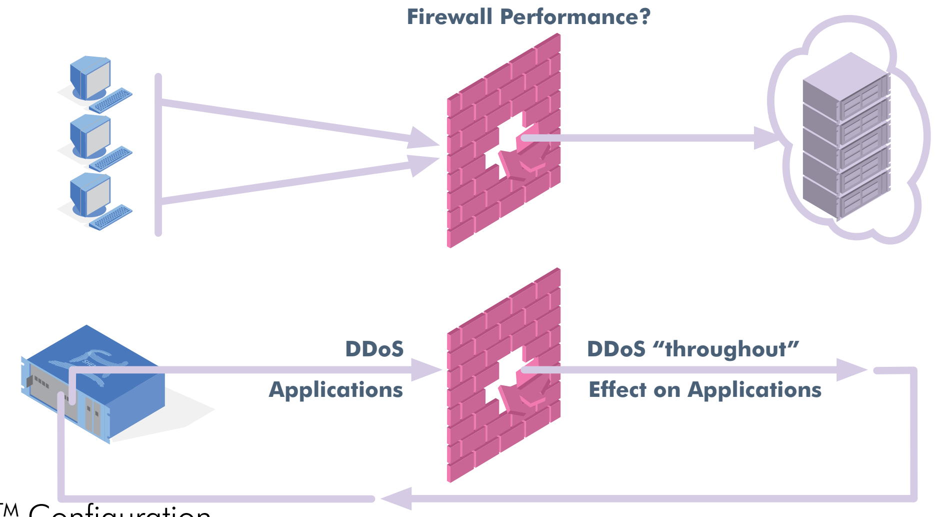
REALITY CHECKED™ SHENICK

Sample Security Attack Test Scenarios

Firewall/IPS/IDS performance and quality of experince test under regular and Security attack conditions. Test connections per second, sustained connections, throughput, loss, delay and jitter on a per application basis. Determine the effect of an attack on quality of experience (QoE) with a mix of legitimate and malicious traffic within converged IP networks. For example, per viewer IPTV video quality, VoIP call quality, Web response times etc.

Determing effect on IPTV QoE during security attacks. With firewalls and other attack mitigation devices forming an important part of triple play access infastructure, assess the effect of a DDoS attack or multicast specific attacks such as IGMP Membership Report Flood on IPTV quality of experience for video and TV channel zapping.

Test performance of Email Servers/Anti-Virus Systems, Anti-Spam devices. Generate both regular email and virus/worm laden emails. Determine 'virus throughput' and performance effects under attack conditions. Generate masses of spam and test anti-spam devices.



Sample diversifEye™ Configuration

Software Specification

- **DDoS Attack emulation:**
  - SYN/RST/UDP/ARP floods, Reflective DDoS attacks,Ping of Death, Teardrop. IGMP membership report floods and SIP attacks coming soon!

- **Virus/Worm and Spam :**
  - Full support for email attachments containing either real or disabled viruses on a per email controlled basis. Emulate real spam emails.

- **Regular Client/Server Traffic Generation :**

Triple Play IPTV -	Complete video analysis with MOS Scores. Real time, full reference active (PEVQ) analysis plus passive (VQS) analysis. QoS/QoE metrics. IGMP/MLD zap rate tests.
VoD -	RTSP based streaming support.
VoIP -	SIP/RTP and configurable Codecs.
P2P -	Support for P2P signatures and generation of all P2P protocols e.g. eDonkey, Skype
HTTP -	Web server & Email emulation on an application flow basis.
SMTP -	Including POP3.
Other -	VLAN, DHCP, PPPoE, IPv4/IPv6.
Capture Replay -	PCAP Raw Port Playback and TCP playback.

KEY FEATURES AND BENEFITS

- Determine Security and Performance Bottlenecks.
- Find out real world performance limitations under normal operation and/or attack conditions.
- Generate regular (internet mix of HTTP, email, streaming, multicast) and attack traffic (DDoS, Virus, Spam) at the same time.
- Determine attack throughput rates.
- Find out the effect on typical regular end user QoE (Quality of Experience) before, during and after attack.
- Support for email attachments including Viruses (both safe mode and real).

Europe | Brook House, Corrig Avenue, Dun Laoghaire, Dublin, Ireland. **Tel:**+353-1-2367002 **Fax:**+353-1-2367020
North America | 533, Airport Boulevard, Burlingame, CA, 94010, USA. **Tel:**+1-650-288-0511 **Fax:**+1-650-745-2641
web: www.shenick.com **email:** info@shenick.com