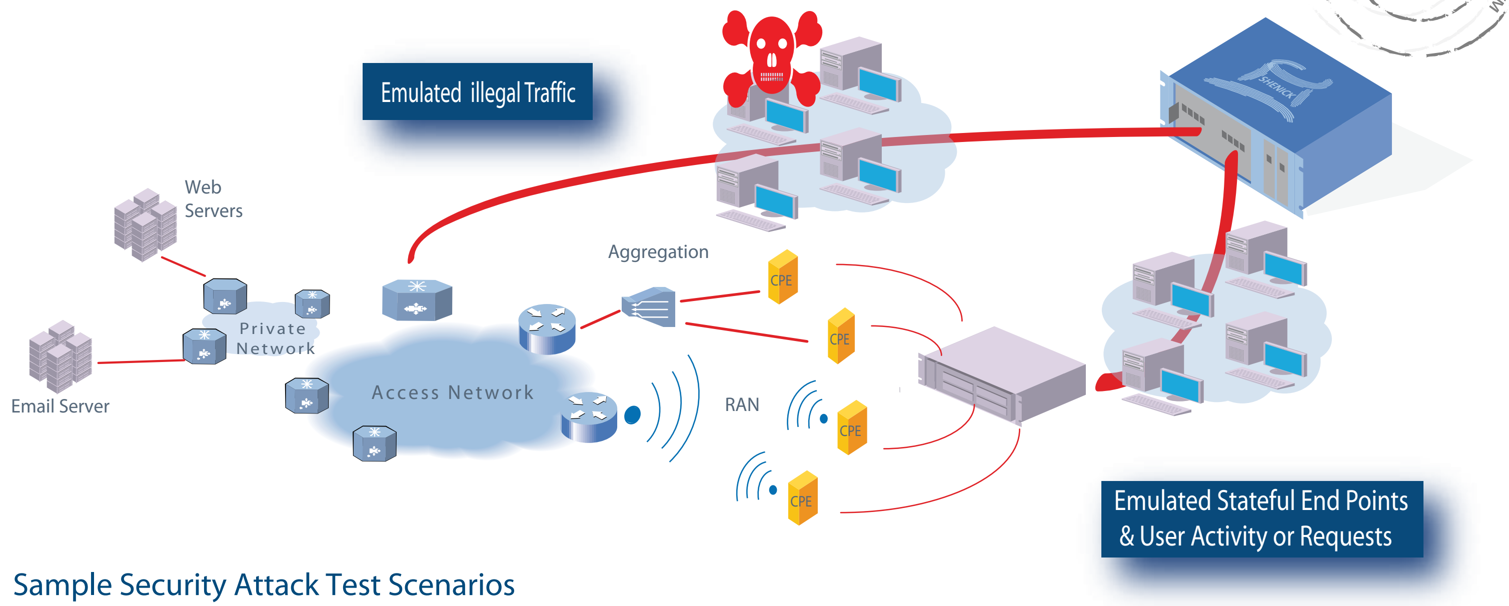
SHENICK

Testing Security of IP Networks with diversifEye™

As the number of attacks on IP networks and networked devices increase and become more sophisticated, un-quantifiable sums of money are spent annually on securing facilities and data. Cyber crime continues to evolve, with attack types ranging from sabotage to malicious content such as viruses and worms, distributed denial of service (DDoS) attacks as well as the proliferation of Spam.

Is this money well spent? The alternative is a successful DDoS attack, resulting in a loss in business, revenue and more importantly a loss in business confidence. How secure is secure? To successfully evaluate the usefulness of next generation cyber crime mitigation technology and solutions requires real world scenarios. To deliver these unique terrifying traffic flows requires a per flow solution, diversifEye.

REALITY CHECKED™ SHENICK



Sample Security Attack Test Scenarios

Firewall/IPS/IDS performance -
Examine quality of experience under regular and security attack conditions. Test connections per second, sustained connections, throughput, loss, delay and jitter on a per application basis.

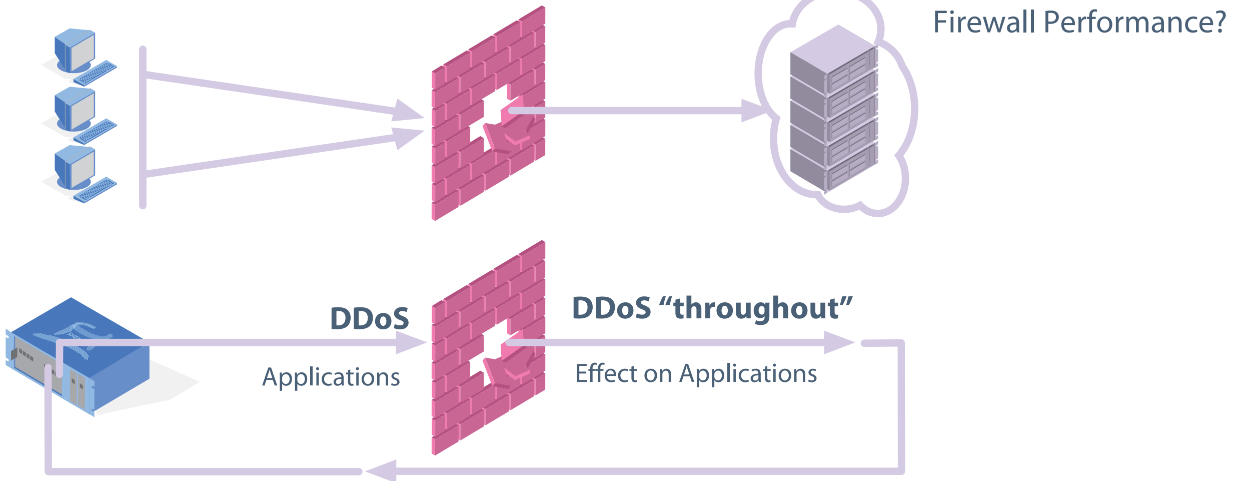
Testing for false positives -
Out of the mass of daily emails / uploads, can the security system identify the one possible illegal flow with an illegal attachment correctly?

Determine the impact on subscription content such as IPTV during security attacks -
Firewalls and other attack mitigation devices form an important part of securing infrastructure, 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.

Cyber crime may be classified as visible or invisible. The visible threat is one in which the network or a device on the network is targeted for some unlawful gain. Visible threats exploit the "Openness" of IP networks and systems. Invisible threats use network resources to facilitate crimes in the real world. In both instances testing the devices that secure the network or facility requires a Per flow approach, delivering unique flows and application activity e.g. a single email with a map attachment or requests to web servers with illegal attachments.

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.
- 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. Support HTTP POST with multiple content types.
- Real world attack conditions :
  - 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.
- Regular Client/Server Traffic Generation :
  - Triple Play IPTV - Complete video/audio analysis with MOS Scores.
  - Telepresence - Quad-flow emulation & measurements.
  - 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 and Email emulation on an application flow basis.
  - SMTP - Including POP3.
  - Other - VLAN, DHCP, PPPoE, IPv4/IPv6, Dual-Stack Lite.
  - Capture Replay - PCAP Raw Port Playback and TCP playback.

diversifEye Summary Features and Benefits

- Network QoS and per flow QoE granularity for individual emulated flows across multiple devices and triple play application types.
- Latest protocols and features supported from IPTV (IGMP/MLD), VoD (RTSP), VoIP (SIP/RTP), Telepresence, Data Applications (HTTP, FTP, POP/SMTP, P2P) all in a single test package.
- Voice and Video / Audio Analysis supported.
- 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 intelligent PCAP replay for Instant Messaging, Web Mail or Internet Gaming.
- TCP Replay Substitution automatically varies payloads so no two PCAP sessions are the same, ideal for QoS tests.
- 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.

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