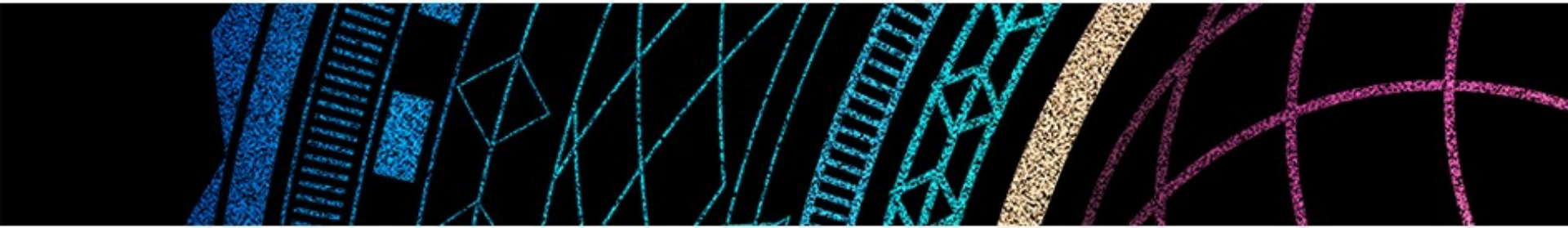
运营商网络安全测试方案

测试实例剖析和测试方法



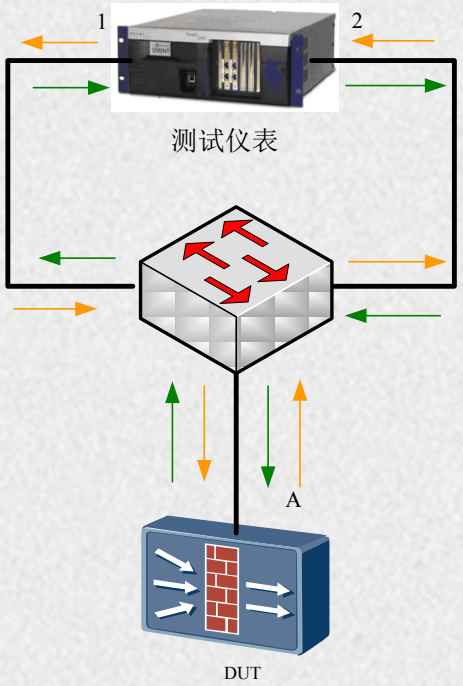
敏捷已来

Weaving The Future

Envision A Better Connected World

议程

- 运营商网络安全测试案例分析
  - 防火墙测试
  - IPS、DPI测试
  - P2P应用流量测试
  - CR协议健壮性测试
- 运营商网络安全测试方法总结
- 思博伦在网络安全测试领域的进展



测试实例1 – 防火墙测试

- 运营商防火墙测试的趋势
  - 单纯的性能测试（基于RFC 3511）不再是运营商测试的唯一目标
  - 基于HTTP的测试，向多种业务综合测试发展，HTTP+FTP+MAIL+其它应用…
  - 测试设定条件更为严格，更贴近现网的某些配置或者基于现网的配置策略，从采用真实报文大小，到更真实的报文内容，到单连接多事务处理数量，等
  - 单性能指标测试向指标集成测试（新建、并发、带宽指标互为背景的测试）发展
  - 多业务、多应用混合的稳定性测试
  - 针对防火墙增值能力的扩展或下一代防火墙的发展，对于各类应用的DPI能力测试
  - IPSec能力测试
  - 防火墙抗攻击能力测试，攻击流量识别，健壮性测试

运营商防火墙测试条目举例

测试条目	测试目标	Layer	重要程度
并发测试（以新建为背景）	测试用户并发容量 验证20%新建速率是否影响并发容量，验证条件： • 工作在NAT模式 • 测试内容为512K以上，真实录制的现网网页内容 • 验证重叠、乱序包能正确处理	L4-7	Yes
新建测试（以并发为背景）	测试新建速率性能 验证20%并发用户背景是否影响用户新建速率，验证条件同上	L4-7	Yes
有效流量（混合新建、并发）	根据现网统计模型，构造并发，新建和有效流量并存的测试	L4-7	Yes
多种应用流量模型测试	测试防火墙在一定规则条件下，对多种应用流量混合流量的处理能力，比如HTTP : FTP : MAIL = 7 : 2 : 1	L4-7	Yes
IPSec测试	测试防火墙IPSec隧道容量，IPSec隧道新建速率，IPSec流量处理	L3-7	Yes
新应用识别能力	对启用DPI功能的网元，测试应用识别能力	L4-7	Optional

严格的测试条件

- 原则上测试过程中不允许重启
- 测试预置条件验证

1) 被测防火墙工作正常；

2) 配置被测防火墙：

配置被测设备端口 A 的 IP 地址为 210.135.1.1/16；端口 B 的 IP 地址为 210.136.2.1/16；

配置被测设备工作在“NAT 模式”，使用“端口 NAT”（M:N，N>1），并且 NAT 地址池大小为 1000：210.136.2.11-210.136.2.210、210.136.3.11-210.136.3.210、210.136.4.11-210.136.4.210、210.136.5.11-210.136.5.210、210.136.6.11-210.136.6.210；

按照统一提供的模板配置 101 条安全防护策略（见模板）；

开启 NAT 日志记录功能，SNMP 管理功能；启用分片包处理机制；

使能 ALG 功能（SIP、RTSP、FTP）；

3) 配置测试仪表仿真服务器：

测试仪表端口 2 模拟 HTTP Server，地址为 210.136.2.2/16；

服务器端 Latency 设为 0ms，页面为 8bytes 的静态页面；

4) 配置测试仪表仿真客户端：

测试仪表端口 1 必须启动“虚拟路由器（VR）”功能，VR 地址为 210.135.1.200/16，默认路由指向 210.135.1.1，禁止仿真的客户端 IP 与被测设备端口 A 同一网段或直连；

测试仪表端口 1 模拟 6 个客户端（地址分别为 192.10.1.0/24、

预置条件和测试步骤

- 严格的测试步骤和预期结果

预期结果:	1) 步骤 1 中的所有安全防护策略验证成功； 2) 步骤 2 中重叠分片数据包被丢弃，乱序分片数据包被正确排序后发送到端口 2，SIP 和 HTTP 业务均成功； 3) 在服务器侧抓包分析，验证所有业务请求均 NAT 生效； 4) 业务成功率必须大于 99.0%； 5) 查看被测设备 session 表和 NAT 日志及数量； 6) 测试过程中设备禁止重启，如遇特殊条件（死机等），记录重启和死机次数。

	192.11.1.0/24、192.12.1.0/24、192.13.1.0/24、192.14.1.0/24、192.15.1.0/24)； 需在被测设备上配置回程路由，192.0.0.0/8 下一跳为 210.135.1.200。 配置前 5 个客户端 Action 为 HTTP GET,且每一个 Connnection 中只有一个 Transaction，即只有一个 GET。最后一个客户端模拟 100 个用户,持续进行 http 下载(Http Get 的页面大小为 1MB 的静态页面)，总流量需达到设备所属典配流量模型要求的 20%。 且由于 avalanche 仪表上的 ACL 验证模板使用的是 190.0.0.0/8 的源地址进行访问，所以同样需要对这个网段配置回程路由，190.0.0.0/8 下一跳为 210.135.1.200
测试步骤:	1) 配置仪表，端口 1 发起一种或多种业务请求，验证之前配置 101 条安全防护策略生效； 2) 端口 1 向端口 2 发送重叠分片数据包、乱序分片数据包、SIP 业务流量，同时发送新建速率为 2000/s 的正常 HTTP 连接； 3) 停止步骤 2 中的所有流量，配置仪表端口 1 的前 5 个客户端发起 HTTP 业务请求（匹配允许的安全防护策略），测试被测设备设备支持的最大新建连接数（稳定值，瞬时峰值无效），达到最大压力后保持压力 10 分钟； 4) 记录被测设备支持的最大新建连接数。

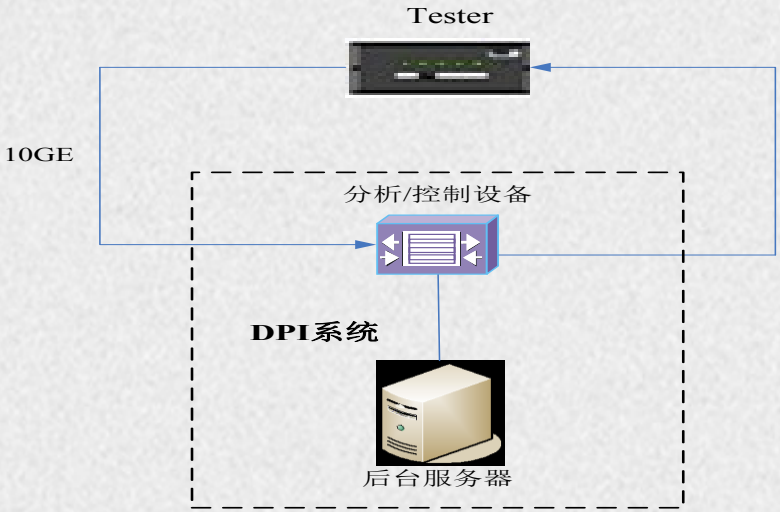
运营商防火墙测试小结

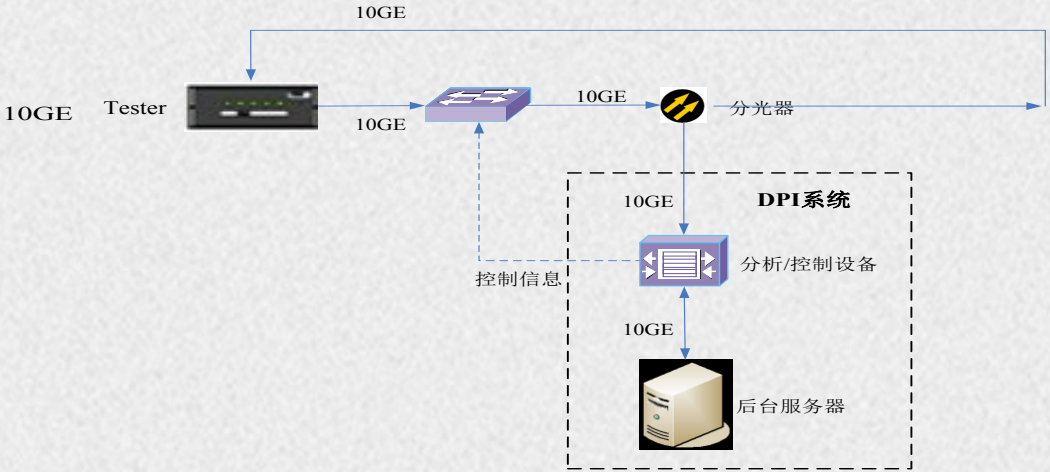
- 在预置条件多，要求严格的情况下，Avalanche能够很好地实现测试要求
- 运营商测试会更多地倾向于在指标测试的基础上，增加背景更接近现网的实际情况，这一点对于Avalanche实现而言非常简单、方便
- 对于多种应用混合的模型，Avalanche基于现有的协议实现可以比较快速的模拟，不会局限于自己内嵌的固定模型
- Avalanche在测试统计的丰富性、准确性等方面是有很大优势的，包括实时结果和测试后的结果分析

测试实例2 – IPS、DPI测试

- IPS、DPI项目背景
  - IPS、DPI系统做为运营商进行IP业务流量监控的一种辅助手段，主要目的包括：流量管理，精确流量计费，网络服务差异化，内部运营支撑，增值业务
- 测试内容
  - 全业务分析与控制功能
  - 隧道流量识别与控制功能
  - 一拖N检测与控制（真实环境测试）
  - DDoS异常流量分析与控制
  - 用户行为分析与控制
  - 被测系统分别对P2P下载流量进行识别、统计，包括P2P下载流量对应的软件名称、不同应用的流量及流量占比，记录单业务数据流识别误差率，记录统计结果

DPI测试拓扑图


Tester
10GE
分析/控制设备
DPI系统
后台服务器


10GE
Tester
10GE
10GE
分光器
10GE
DPI系统
分析/控制设备
控制信息
10GE
后台服务器

实际测试举例

- 在本次测试中，被测设备基于处理能力被分为4档：
  - A档 8G应用层处理能力，新建连接速率>12万，并发>600万
  - B档 4G应用层处理能力，新建连接速率>6万，并发>300万
  - C档 2G应用层处理能力，新建连接速率>3万，并发>200万
  - D档 1G应用层处理能力，新建连接速率>1.5万，并发>100万
- 测试用例
  - 性能测试：TCP新建连接速率（CPS）、并发连接数、QPS
  - 应用保护能力测试：公开漏洞检测、异常协议检测、权限获取、蠕虫事件、缓存区溢出、注入、xss、IPS逃逸
  - 其它测试：误报漏报测试；带宽管理；URL过滤功能

运营商IPS、DPI测试小结

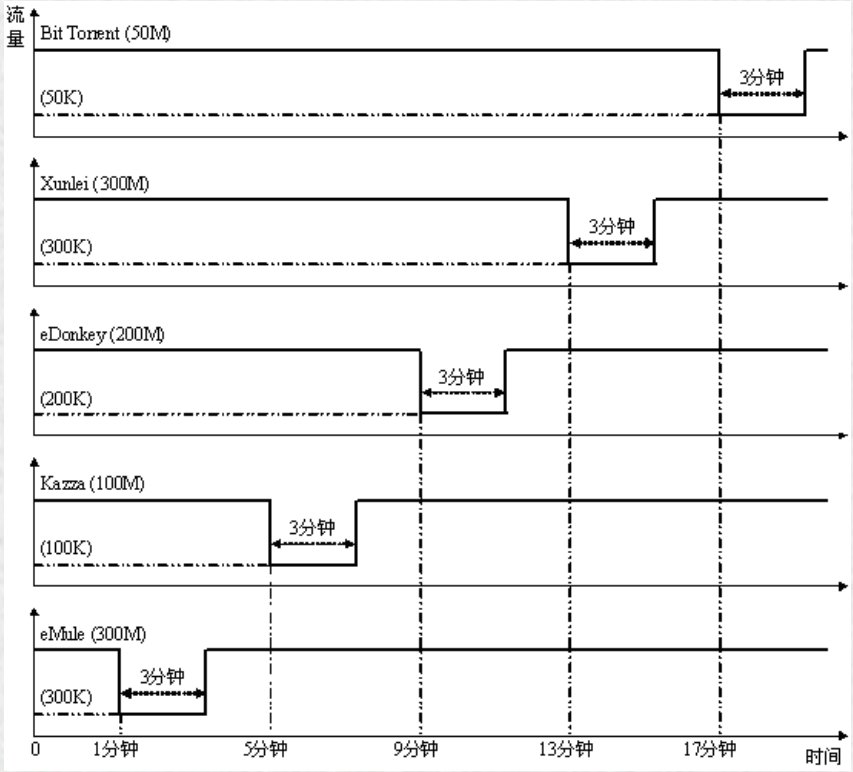
- 通过运营商IPS、DPI测试，基本上拿到国内最常见应用的流量模型，而且是经过多个厂商设备验证过含特征码的流量模型，基于此建立了运营商应用库
- 主要包括以下应用业务模型：讯雷、PPStream、QVOD、QQLive、BitTorrent、风行、暴风影音、FlashGet、酷狗、PPTV、旋风、9158、呱呱聊天、FlashStreaming、优酷、Skype、QQ、LAVA、YY、阿里旺旺、MSN、QQ游戏、天龙八部、大话西游、浩方、天堂，等
- 测试内容具有广泛的代表性，所有应用均通过SAPEE来导入仿真
- 由于测试内容和应用的实时性以及流量模型的周期变动性，很难用固定的模型来验证，需要仪表随时支持最新的应用，构建最新的模型，Avalanche可以很好的处理这些变化

测试实例3 – P2P应用流量测试

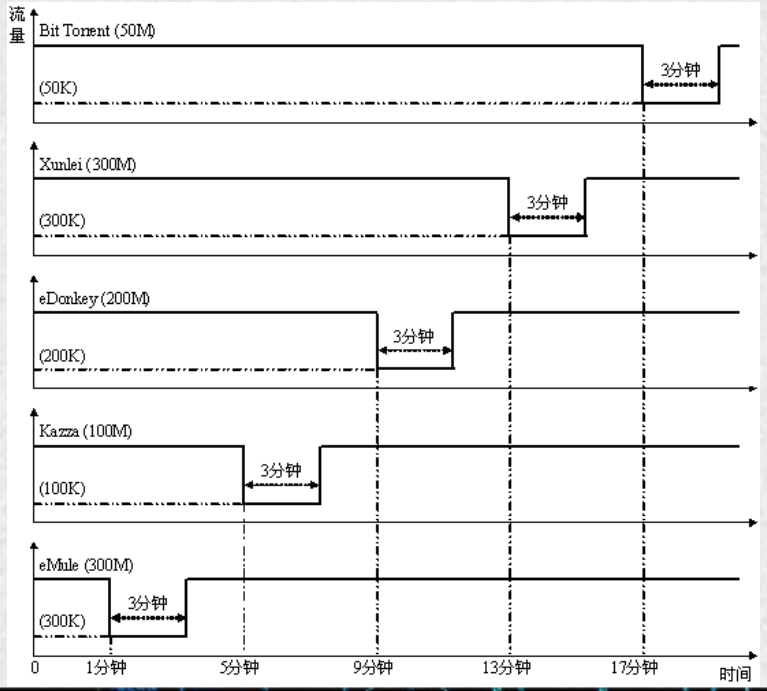
- 被测设备是P2P监控及流控系统，要求被测设备要保证转发大流量P2P协议（超过900 Mbps），必要时对P2P进行流量控制要准确、有效
- 3大类P2P流量仿真（总共15种P2P应用）
  - P2P文件下载（BitTorrent、eDonkey、eMule、Kazaa、迅雷）
  - P2P即时聊天（MSN、Yahoo Messenger、QQ）
  - P2P流媒体（PPStream、PPLive、QQLive、UUSee、TVKoo、原力、上海网用）
- 高性能要求（单个千兆测试口需要模拟超过900 Mbps的P2P流量）
- 多种P2P流量混合测试
- 需要同时模拟基于TCP和UDP的P2P应用

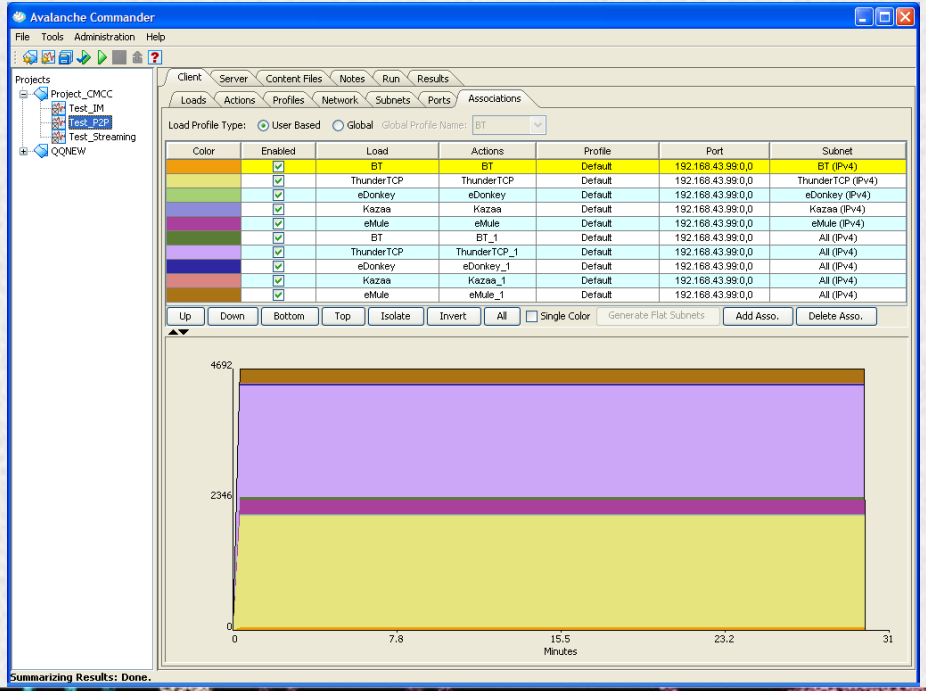
P2P文件下载流量模型

测试要求：测试开始的1分钟，观察DUT是否能够正常转发900 Mbps以上的混合P2P流量。1分钟之后，DUT对应用1进行3分钟的流量控制（1000分之一），看DUT是否控制准确（协议、流量）。3分钟后取消流控。再1分钟后，对应用2进行3分钟的流量控制。以此类推，直到对所有应用都进行一遍3分钟的流控。观察测试期间DUT对P2P应用流量的监控和流控的性能



P2P文件下载应用流量实现





P2P应用流量测试小结

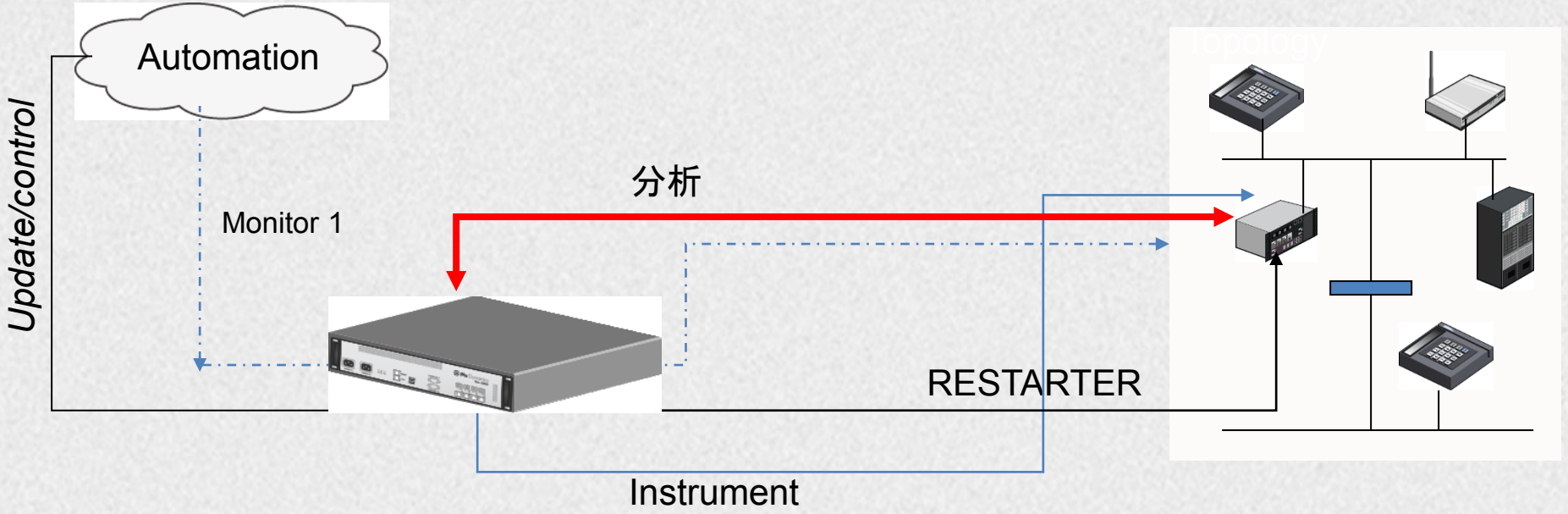
- 高性能 – Avalanche单个GE端口可以模拟超过900 Mbps的混合P2P流量
- Avalanche可以为每种P2P协议设置特殊的load profile并且能够准确地模拟每种P2P协议各自的带宽
- 从现网捕捉到的P2P流量是抖动的，但运营商要求Avalanche为每种P2P协议生成恒定带宽的流量，此时Avalanche的Load Profile和Load Constraint发挥了极大的作用，可以很准确地模拟恒定带宽的P2P流量
- Avalanche的SAPEE可以同时模拟TCP和UDP协议
- 只有Avalanche的SAPEE可以进行如此复杂、高性能的P2P测试

测试实例4 – CR协议健壮性测试

- CR健壮性测试背景

- CR本身没有防护能力，而其本身在网络的核心位置
- CR所用协议实现虽然都是成熟的协议，但是在各种测试中却很少涉及对其安全进行测试
- 一些针对路由器的安全攻击也时有发生
- 一些网络防护设备无法对路由器的异常报文攻击进行有效的防护
- CR本身实现的健壮性是保证网络安全的基础

CR协议健壮性测试拓扑图

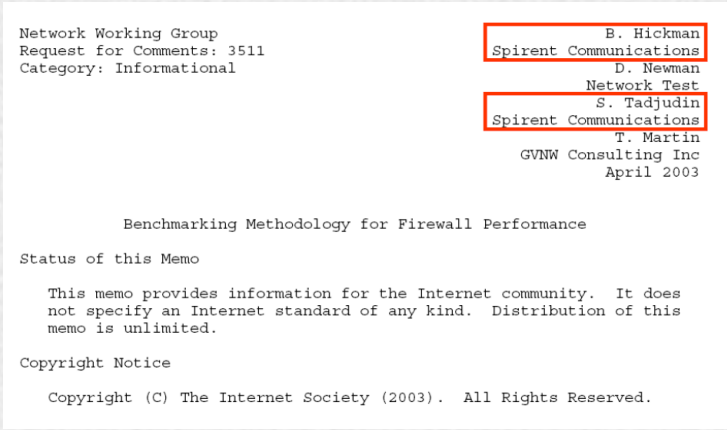


CR协议健壮性测试小结

- 从2013年开始，CR测试加入了协议健壮性测试
- 健壮性测试主要评估CR路由协议对于异常输入的处理方式
- 主要测试协议包括BGP4+， OSPFv3
- 测试发现问题
  - BGP4+总共4360个测试例，发现漏洞23
  - OSPFv3发现漏洞24个，其中约有10个左右的漏洞会导致OSPF进程挂死

运营商网络安全测试方法总结

- 基准性能测试基于RFC 3511（最基本要求）
  - 并发连接数、TCP连接建立速率、Goodput
- 攻击仿真测试
  - 高性能DDoS测试、已知攻击仿真测试
  - Malware测试
  - 协议健壮性测试 – Fuzzing测试
- 攻击手法升级方法
  - 提供及时、周期性更新的攻击手法库，有需要去下载更新 – Knowledge Base订阅服务
  - 客户化定制攻击手法 – Attack Designer



Network Working Group
Request for Comments: 3511
Category: Informational

B. Hickman
Spirent Communications
D. Newman
Network Test
S. Tadjudin
Spirent Communications
T. Martin
GVNW Consulting Inc
April 2003

Benchmarking Methodology for Firewall Performance

Status of this Memo

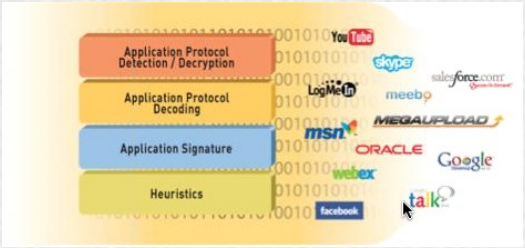
This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

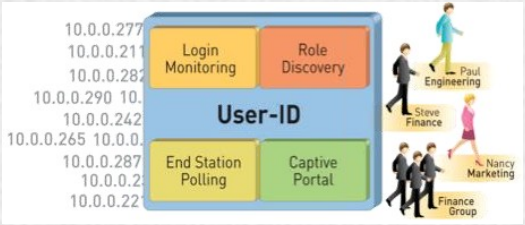
Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

运营商网络安全测试方法总结（续）

- 对各种流行应用的真实性模拟
  - 流行应用种类繁多
  - 同一应用有不同版本和行为
  - 各种应用混合下的性能测试
  - 应用和攻击流量混合测试
- 应用测试实现方法
  - 提供及时、周期性更新应用库，有需要去下载更新 – TestCloud库
  - 提供一个工具，按照需要生成最新的应用，并以此建立应用库 – SAPEE





运营商网络安全测试方法总结（续）

- 云安全测试 – 虚拟化
- 加密协议测试
  - IPSec VPN测试 – 并发IPSec隧道数、IPSec隧道建立速率、IPSec隧道吞吐量
  - HTTPS/SSL性能测试、SSL VPN测试
- 网络中真实性模拟测试
  - 动态地址分配：DHCP、PPPoE
  - 网络损伤模拟：丢包、延迟、抖动，等
  - IP分片
  - IPv4/IPv6：NAT64、DS-Lite、6RD，等
  - GTP、GRE、虚拟路由模拟，……

思博伦在网络安全测试领域的进展

- 思博伦拥有防火墙性能基准测试标准RFC 3511

- 思博伦安全测试相关的合作伙伴
  - NSS – Hypervisor测试， WAF测试
  - UNH – 美国政府NPD认证测试
  - ICSA – 与R-scope合作的100G测试，NPD测试
  - Network Test
  - Mantech Cyber Range
  - Cybersecurity

Avalanche NEXT – 赢得Best of Interop大奖

- Interop, Las Vegas, NV – 2014年4月
- 获奖类别：Performance
- 视频采访
  - http://vimeo.com/91417855

Spirent Avalanche NEXT Wins Best of Interop 2014 Award

Apr 4, 2014

Spirent solution recognized for making application performance load testing capabilities accessible for traditional IT

Sunnyvale, Calif. – April 7, 2014 — Spirent Communications, a leader in testing networks, services and devices, announced today that Spirent Avalanche NEXT has won the Best of Interop 2014 Award in the Performance category. According to the judges, Avalanche NEXT won because it delivers application performance testing capabilities into the realm of traditional IT.

"Performance load testing has historically been a complex and costly process, because building and verifying the test bed, defining the tests, and interpreting the results required expertise in a variety of disciplines," said Mike Fratto, Principal Analyst at Current Analysis and Best of Interop Judge.

业内领先 – 测试方法学和公开测试

BYOD: The Hidden Threat

A Spirent White Paper

Irrespective of whether corporate policy allows BYOD, as a 2013 Ovum employee study shows, more than sixty percent of employees bring in their own devices (smartphones, tablets, and personal laptops) and access corporate resources with them. The report reveals that 67.8 percent of those who own a smartphone bring it to work, 15.4 percent without the IT department's knowledge and 20.9 percent in spite of a published anti-BYOD policy.

BROADBAND TESTING

Can Security Testing Be Simple?

A Report of Spirent Avalanche NEXT Featuring Next Generation Firewall

White Paper

Impact of NIST Cybersecurity Framework on Service Providers, Enterprises and NEMs

RSA Conference Asia Pacific 2013 — 新加坡

结束语

- 网络安全问题越来越得到运营商的重视，每年各大运营商都会组织各种安全设备（防火墙、IDS/IPS、DPI、VPN、P2P，等）的集采测试、入网测试等
- 思博伦每年协助各大运营商完成诸多网络安全测试项目
- 思博伦Avalanche提供业内最高性能的应用和安全测试方案
- 提供数千种应用测试场景，并提供基于SAPEE的特殊应用定制
- 提供包括Malware、Fuzzing以及已知攻击等全面攻击测试解决方案
- 思博伦对攻击流量和应用流量的仿真，都提供定期更新的数据库，以及客户定制化工具，既能满足对最新应用及攻击的支持，又能满足用户的特殊要求
- 加大对安全测试的研发投入，为广大用户提供最好的网络安全测试方案

HUAWEI

SPIRENT

谢谢

敏捷已来

Weaving The Future

Envision A Better Connected World