Avalanche介绍

孙磊 13611133940
Lei.sun@spirent.com

Avalanche介绍

全面的应用和安全测试解决方案

- 全面的应用与安全测试解决方案
- 多平台支持
  - C100-MP、C100-S3、CF20、C1
  - CyberFlood Virtual
  - TestCenter
  - 支持1G到100G接口
- 优势：
  - 广泛的用户基础
  - 支持单臂和双臂测试
  - 功能丰富
  - 高度灵活性
  - 性能强劲
  - 支持网络安全测试

典型客户列表

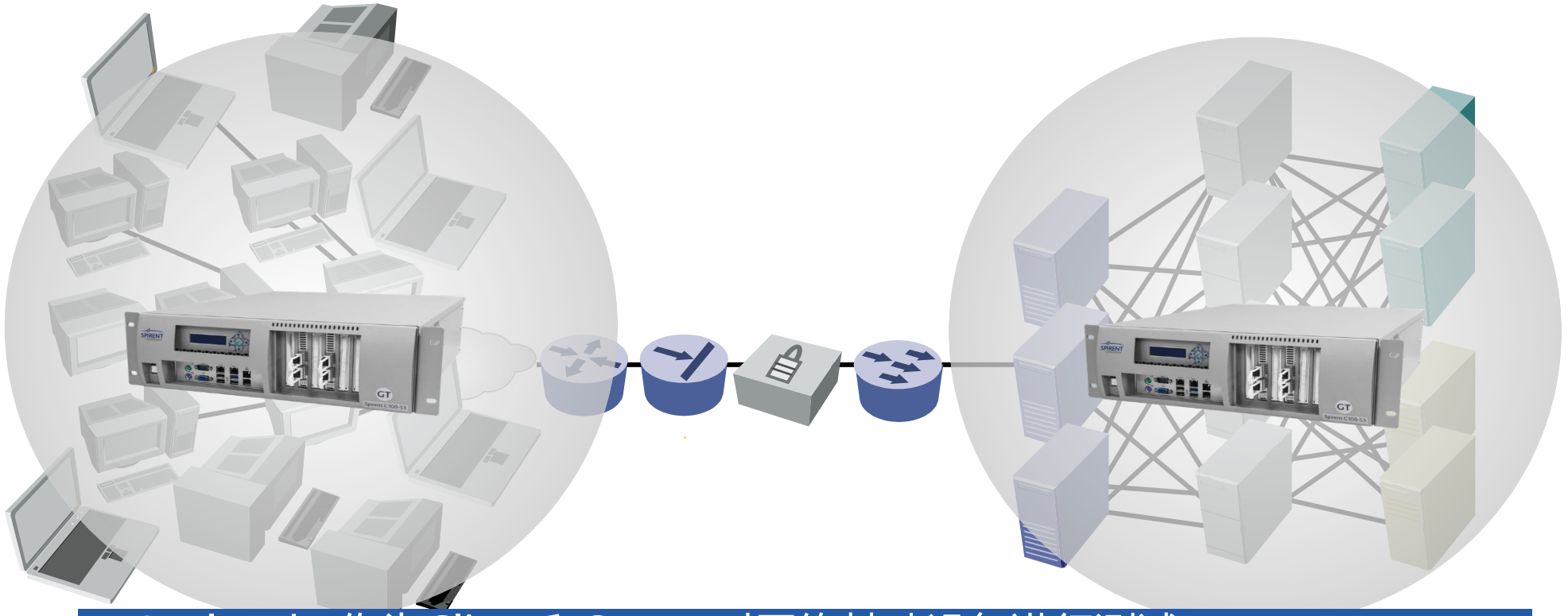

f5
ERICSSON
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
Juniper NETWORKS
NTT
UNITED STATES MARINE CORPS
TSINGHUA 1911 UNIVERSITY
PEKING UNIVERSITY 1898
ZHEJIANG UNIVERSITY 1897
and 和
中国移动 China Mobile
中国电信 CHINA TELECOM
Check Point SOFTWARE TECHNOLOGIES LTD
Sprint
SOURCEfire
NANJING UNIVERSITY 1902
1958
USTC 1956
vmware
Alcatel·Lucent
CISCO
ARUBA networks
MITRE
Redback NETWORKS
BROCADE
BROADCOM
verizon
EQUINIX
at&t
T-Mobile
SoftBank
Comcast
McAfee Proven Security
hp
中国建设银行 China Construction Bank
ARRIS
Honeywell
H3C 数字化解决方案领导者
bright house NETWORKS
intel
RBS
invent JPMORGAN CHASE & CO.
NetApp
COX COMMUNICATIONS
HUAWEI
ABB
FORTINET
U.S. AIR FORCE
paloalto NETWORKS
TELUS
U.S.ARMY
Deutsche Bank
netmarble
AVAYA
BT
SIEMENS
GENBAND
ciena
BOEING
Symantec

Avalanche协议和功能支持覆盖

- Avalanche 基础：HTTP，FTP，DNS，Telnet
- 邮件： SMTP/POP3/IMAP4, ESMTP/POP3 over SSL/IMAP4 over SSL
- 音频视频：RTSP/RTP/RTCP, RTMP/RTMPT,MMS, HTTP/HTTPs ABR, DASH, 4k, SIP over TCP/SIP over UDP, IGMPv2/IGMPv3/MLDv2
- 接入网：DHCP，PPPoE，RADIUS，802.1x/NAC
- 加密：IPSEC（IKEv1，IKEv2），SSL（SSLv2，SSLv3，TLSv1, TLS1.2, TLS1.3）
- 存储：CIFS,NFS
- 模糊测试：健壮性测试，鲁棒性测试
- 报文回放：SAPEE支持P2P, 网盘,和TCP/UDP私有协议测试，支持国内外流行的应用（即时消息如微信，抖音，QQ，斗鱼等）
- 隧道协议：GTP，GRE
- 新协议：HTTP/2，QUIC
- IPV6：IPv6，DSLlite，6RD
- 网络安全：漏洞攻击，DDoS，僵尸蠕虫，木马和勒索软件

Avalanche测试应用场景

网络设备及网络基础架构测试

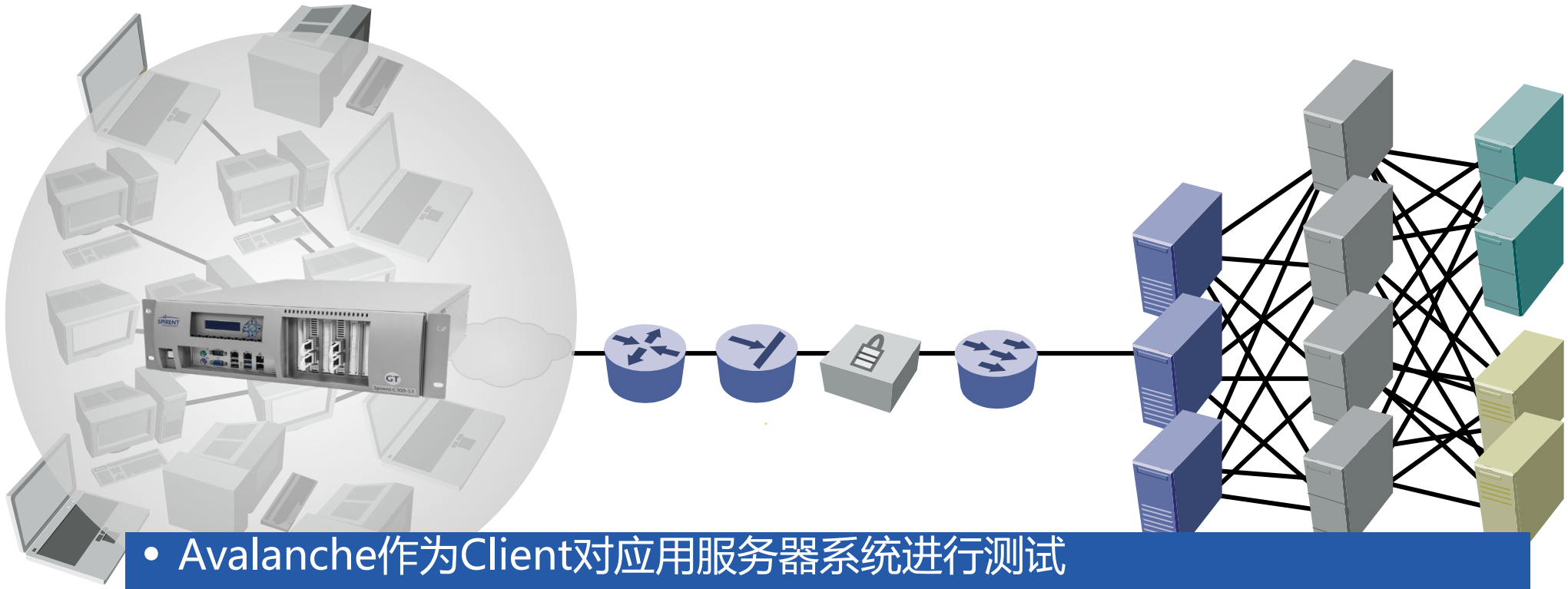


- Avalanche作为Client和Server对网络基础设备进行测试
- Avalanche 仿真真实用户行为，发起持续的网络应用服务
- Avalanche物理端口仿真多种应用服务器。
- Avalanche混合各类应用服务以及网络攻击，组合现网抽象的流量模型。

Avalanche网络设备和基础架构测试

- Avalanche支持以下网络设备的功能和性能测试：
  - 防火墙、DPI、UTM，NGFW，WAF
  - IDS/IPS
  - VPN设备（IPSec VPN、SSL VPN）
  - 应用层交换机
  - 负载均衡设备
  - 网络缓存（web缓存，CDN，P2P缓存）
  - 垃圾邮件过滤系统、防病毒系统
  - 流媒体平台测试（RTSP/RTP、MMS）、IPTV测试、VoD组播测试、移动流媒体测试，渐进式流媒体测试，自适应流媒体测试。
  - NAT444，NAT64，PAT，ALG测试
  - DPI/敏感词/合法拦截
  - 代理服务器及其它应用网关等网络设备
- IPv6网络设备测试

应用服务器系统测试（Client Only）



- Avalanche作为Client对应用服务器系统进行测试
- Avalanche从用户体验的角度对服务器进行测试，特有的动态内容支持可以对诸如网站服务，防盗链，DNS，流媒体服务器等进行测试。
- Avalanche支持通过DHCP，PPPoE，SSL，IPSEC等接入或者加密方式对服务器进行测试。

Avalanche服务器测试

- Avalanche支持以下服务器测试
  - 基于WEB的服务器测试，比如网银测试（SSL），购物网站测试，政务网站测试
  - 网络存储测试（CIFS，NFS，FTP，HTTP）
  - 邮件服务器
  - 流媒体服务器
    - RTSP/RTP（电信，联通，移动，广电CDN测试）包括视频质量解析测试
    - Progressive媒体流测试服务器，比如Youku/Tudou
    - 自适应流媒体服务器测试（Apple，Microsoft，Adobe）
    - 组播测试IGMP/MLD
  - DNS（TCP，UDP/DNSSEC）
  - RADIUS/802.1X
  - DHCP/PPPoE
- IPv6网络设备测试

Avalanche典型测试场景

建行网银测试

- **测试内容**
  - 网银系统支持用户容量测试
  - 网银系统支持用户接入速率测试
  - 网银系统用户请求事务响应时间测试（一定用户背景和速率情况）
  - 网银流量能力测试
  - 网银系统抗攻击能力
  - 网银系统稳定性
- **Avalanche角色**
  - 作为网银客户发起登录，用户一系列行为仿真，发起退出
  - 仿真大量用户进行容量，速率，流量测试
  - 对于登录过程，用户帐户行为，用户退出过程进行响应时间测试
  - 攻击流量仿真（已知攻击和Fuzzing）
  - 构建大规模用户行为仿真模型，进行稳定性测试

RFC3511防火墙测试

思博伦是防火墙测试标准主要制定者

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.

Avalanche在防火墙测试的领先地位

- Spirent 是RFC3511的主要起草者
- Avalanche具有高性能，可以针对不同测试规模提供的灵活的测试方案
- Avalanche真实完整的协议栈支持，支持任何根据现网提炼的测试项目，包括集成指标测试，流量模型测试
- Avalanche客户端和服务器无耦合性，可以满足任何NAT/ALG等功能和性能测试，并且提供准确的测试结果
- 大规模最新应用支持
- Avalanche是防火墙测试事实上的标准
- 中国移动，中国联通，中国电信，电力系统，研究院所，国家信息安全评测机构，企业网络评测采用Avalanche进行防火墙测试

Avalanche典型测试场景

防火墙测试

- 防火墙测试标准
  - 基准测试标准RFC3511
  - 针对RFC3511标准的缺陷，各重点实验室对RFC3511的补充
- 防火墙测试内容和趋势
  - 指标测试应用现网流量统计模型，从报文内容到报文大小，到单连接事务处理数量
  - 单指标测试向指标集成测试（指标互为背景的测试）
  - 基于HTTP的测试向多业务综合测试
  - 针对防火墙增值能力的扩展或者下一代防火墙的发展，对于各类应用的识别能力测试
  - IPSEC能力测试
  - 防火墙抗攻击，攻击流量识别，健壮性测试

RFC 3511防火墙主要测试条目

测试条目	测试目标	Layer	重要程度
IP Throughput	Determine layer 3 throughput	L2-3	No
TCP并发测试（HTTP/IPv4）	How many open TCP connections can be handled?	L4-7	Yes
TCP新建测试（CPS/HTTP/IPv4）	How many new TCP connections per second can be handled?	L4-7	Yes
Denial of Service Handling	What's the impact of DDoS?	L4-7	YES
HTTP Transfer Rate（Goodput）	Determine layer 7 throughput	L4-7	Yes
Maximum HTTP Transaction Rate	Determine the maximum requests per second rate	L4-7	Yes
Illegal Traffic Handling	Does illegal traffic cause performance drop?	L2-3 or L4-7	No
IP Fragmentation Handling	Does Fragmentation cause performance drop?	L2-3 or L4-7	YES
Latency impact	What is the impact of latency?	L4-7	No
TCP并发测试（HTTP/IPv6）	How many open TCP connections can be handled?	L4-7	YES
TCP新建测试（CPS/HTTP/IPv6）	How many new TCP connections per second can be handled?	L4-7	YES
HTTP Transer Rae（Goodput）（HTTP/IPv6）	What's the impact of DDoS?	L4-7	YES
Max HTTP TPS（HTTP/IPv6）	Determine layer 7 throughput	L4-7	YES

Avalanche应用场景

DPI测试

- 应用为王
- 应用太多，无从知晓明天哪种应用会最流行？
- 应用太多，如何快速仿真？版本太多，如何快速跟进？
- 宣称支持100种应用，那么我需要第101，102种怎么办？
- 是否需要一定等待测试仪表提供最新版本（一般三个月左右）才能进行测试，另外它是否一定提供？
- 两种解决办法：
  - 提供一个工具，我自己生成最新应用，按照我的需要生成自己的库
  - 你提供一个网上周期性更新的库，我有需要去更新

Avalanche应用场景

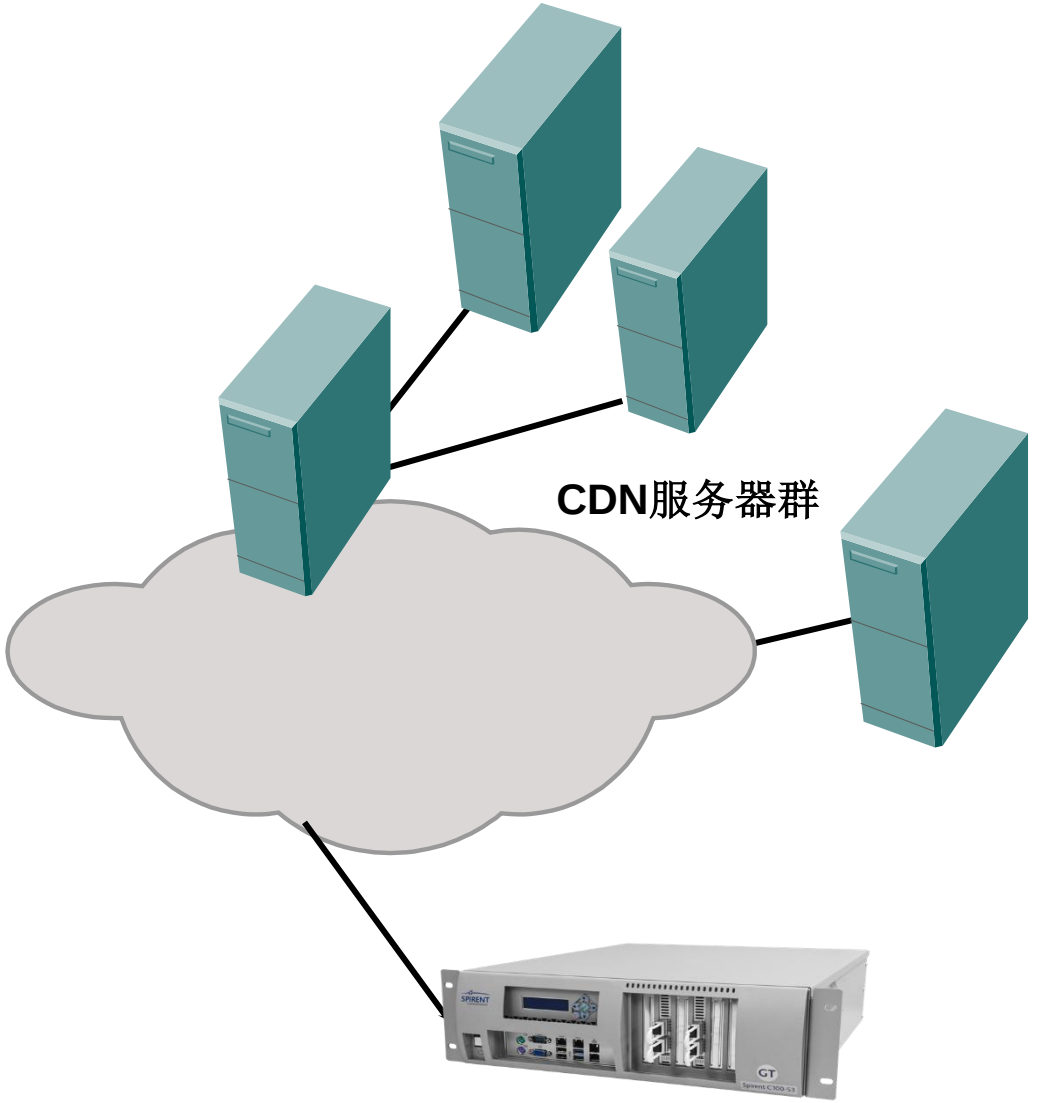
DPI测试

- 北京电信研究院20家DPI测试
- 广州电信研究院DPI测试
- 中国移动DPI测试（8家）
- 中国联通设计院P2P测试
- 传输所DPI测试

Avalanche应用场景

CDN测试

- 最大并发用户
- 最大新建用户
- 最大带宽
- 响应时间
- 长时间稳定性
- 视频质量分析与缓冲分析
- 模拟N用户访问M个内容
- 模拟以二八原则访问热点内容的命中，而不是平均访问的测试
- 100%的流量验证
- 单测试口支持多IP
- 从内容的任意时间开始播放



Avalanche CDN测试

支持的流媒体技术

- 单播RTSP – 电信规范IPTV3.0，Microsoft、Real and QuickTime等客户端
  - RTSP Live streaming
  - RTSP VoD streaming
  - MPEG2-TS over RTP over UDP, MPEG2-TS over UDP
  - RTP over TCP, UDP and HTTP
- 组播流媒体
  - RTP/MPEG2TS
  - UDP/MPEG2TS
  - RTP
- MMS – Microsoft Media Streaming
- RTMP – Adobe Flash streaming
  - RTMP Live streaming
  - RTMP VoD streaming

Avalanche 流媒体测试

- 支持的可选命令
  - PLAY – 播放流媒体文件；
  - PAUSE – 暂停流媒体文件播放若干秒；
  - FF - 快速播放流媒体文件若干秒；
  - RW – 回退流媒体文件若干秒；
  - SEEK – 定位基于偏移量参数的流媒体文件。可以指定从流媒体开始的偏移量秒数。
- 支持任意插入和替换Header
  - 允许用户测试非标准的RTSP实现。用户可以添加（INSERT）/替换（REPLACE）任何RTSP事务中的首部。
  - Range – 设置任意播放的范围，如now-从当前时间开始, end-从最后开始, 或播放从1000到1300秒。
  - Scale – 设置任意播放速度，如+8, -16等
  - 可插入任意其他自定义Header，包括speed, x-cache等

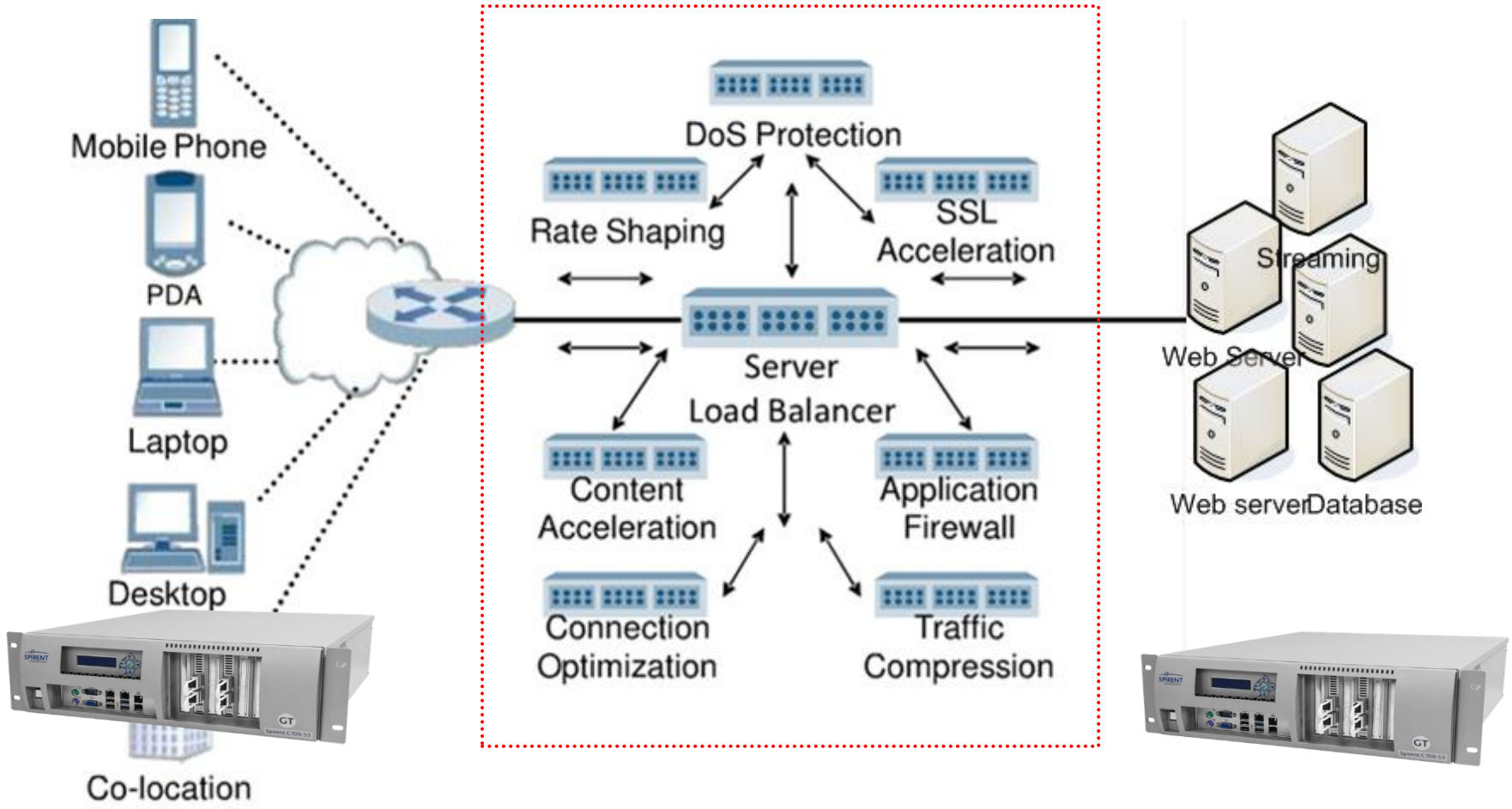
网络攻击和脆弱性评估测试（VA）

- Avalanche 作为攻击方和被攻击方（或者攻击真实服务器）
- Avalanche可以混合攻击流量和正常流量
- Avalanche支持超过10万/秒的有状态（Stateful）攻击
- 攻击流量和正常应用流可以混合通过IPSEC承载
- Avalanche Attack Designer可以自定义新攻击或者攻击变种
- 攻击手法周期性更新反映最新的网络攻击(DDoS,蠕虫，病毒，EMAIL攻击，后门等)

流量模型（Traffic Model）测试

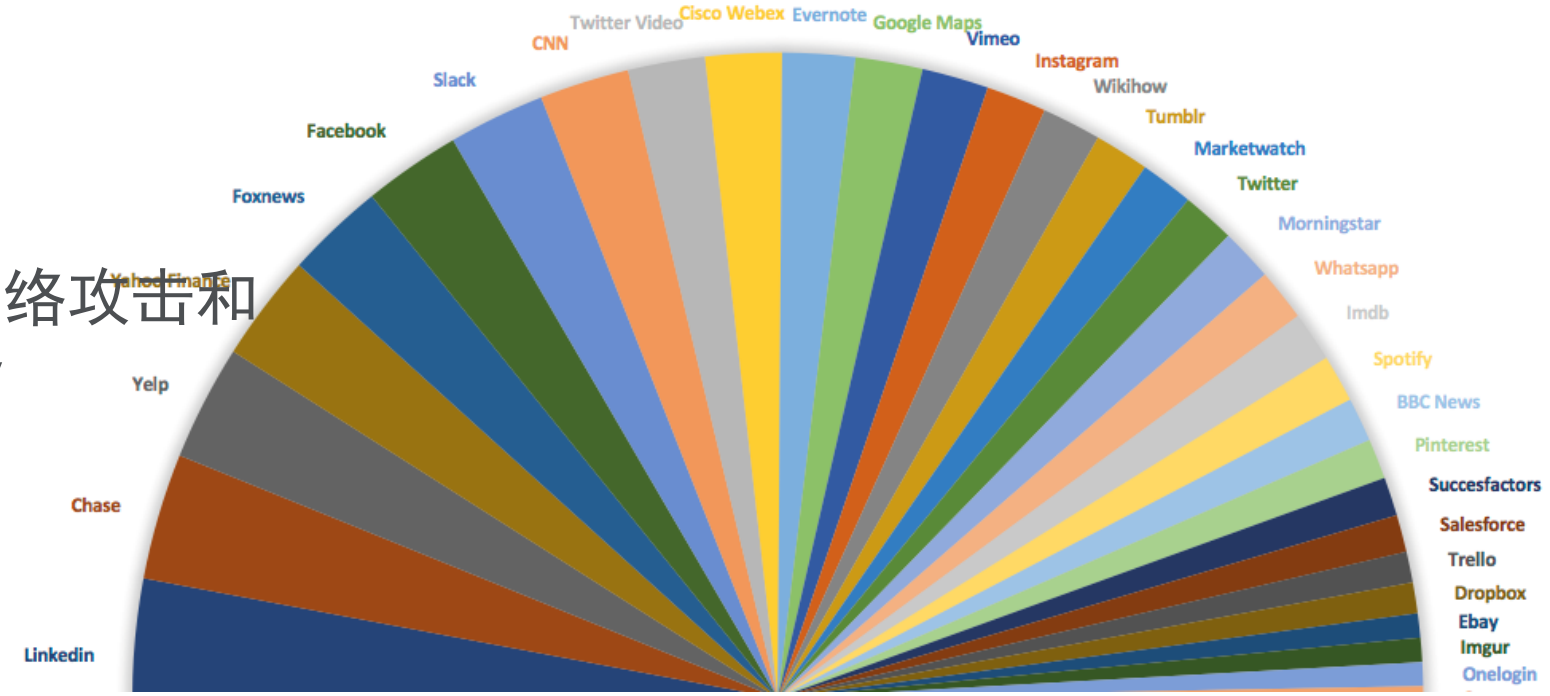
- 流量模型测试必要性
  - 流量模型是对现网运营数据的抽象，反映一段时间内网络流量的分布和特征
  - 流量模型测试对测试仪的要求在于，对各类应用的仿真能力和构建流量模型的能力
- Avalanche流量模型测试
  - 流量可以真实网络场景，需要仿真用户不同接入方式，如PPPoE、DHCP、DNS、802.1x/NAC、Radius、IPSec、SSL、GRE、Virtual routing，等
  - 对于底层承载，可能需要配置ToS & QoS、VLAN、VLAN QinQ、NAT环境穿越、Proxy等
  - 可以加入网络损伤模拟：丢包、延迟、抖动、分片，等
  - 支持真正的Triple Play测试，单端口支持诸如HTTP，Streaming和Voice多种应用服务
  - Avalanche流量模型测试包含网络攻击和漏洞评估测试

流量模型测试场景


Mobile Phone
PDA
Laptop
Desktop
Co-location
DoS Protection
Rate Shaping
SSL
Acceleration
Server
Load Balancer
Content
Acceleration
Application
Firewall
Connection
Optimization
Traffic
Compression
Streaming
Web Server
Web server
Database

支持多种流量模型

- 流量模型中包含常见标准应用，如HTTP、FTP、DNS、流媒体、电子邮件、CIFS，由Avalanche Native Protocol支持
- 模型中的比例关系以带宽（Bandwidth）为基准
- Bad Traffic由Avalanche网络攻击和脆弱性评估（Vulnerability Assessment）功能支持



Quick UDP Internet Connections（QUIC）

- 背景
  - Google发起的UDP通信的改进版
  - 降低网络延时，提高用户体验
  - 5G网络可能会大力推动QUIC使用
- 国内需求
  - 国内在两年前已经有需求，华为在2015年NGFW就支持QUIC
  - 目前实现方式是回放
  - 负载均衡开始支持QUIC，如腾讯云
  - Web服务支持QUIC
- Avalanche QUIC支持
  - 4.87 GA Support
  - Two-arms/one-arm 支持
- Avalanche QUIC TLS 1.3支持
  - 支持TLS1.3
  - 后续支持硬件加速
- 目前唯一支持QUIC的方案

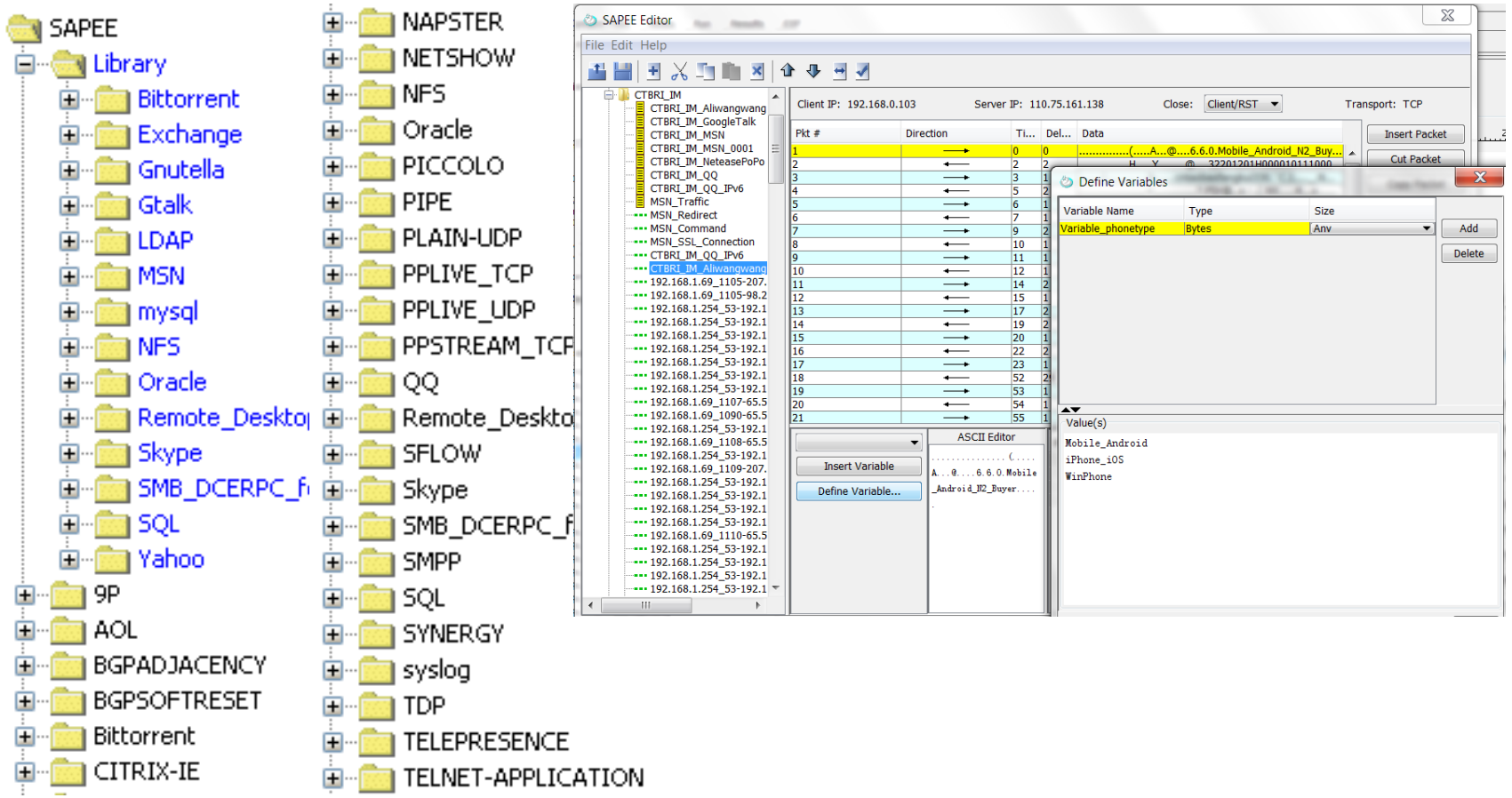
高性能报文回放 SAPEE

- SAPEE提供多流多协议动态协议仿真，支持所有基于TCP/UDP的应用，基于SAPEE可以订制或者自定义任何可重用可编辑的应用协议库，SAPEE是应用生成工具。
- SAPEE回放内容可以100%确保流程的准确性，通过SAPEE你也可以按照自己的要求对内容进行修改，也可以写你自己的私有协议。
- SAPEE支持NAT/PAT测试
- SAPEE支持SSL通道

高性能报文回放 SAPEE

特性

- 支持多种变量
- 支持FormDB
- 支持HTTPs
- 测试MQTT物联网协议
- 测试syslog协议



2018平台一览

cyberflood Virtual	C1	CF20	C100-S3
公有云、私有云 SDN / NFV 功能测试 性能测试 自动化测试	全能小王子 1G/10G测试 支持Avalanche CyberFlood TestCenter	一体式测试仪 高便携 中等性能 1G/10G/40G/100G 内置SSL加速卡	高性能测试 大并发测试 1G/10G/25G 40G/50G/100G 支持SSL加速卡

CF20

CyberFlood	Avalanche	**1U**	内置控制器
SSLVPN加速卡	2x100/40G 8x10G	8x10/1GE	**License bundle**

CyberFlood Virtual

下一代虚拟化方案

CyberFlood Virtual应用与安全的虚拟化解决方案

Avalanche Virtual将被CyberFlood Virtual完全替代

CyberFlood Virtual将同时支持CyberFlood和Avalanche

CyberFlood Virtual

- 性能（每对虚拟端口）
  - 5倍于Avalanche Virtual：10Gbps，50万并发，5万新建
- 目前支持平台
  - VMware ESXi (5.5, 6.0, 6.5)
  - KVM (Ubuntu 16.04 LTS tested)
- 软件支持
  - CyberFlood
  - Avalanche
- 支持云平台
  - Amazon AWS 2018Q4支持
  - OpenStack → 2019Q1
  - Microsoft Azure → 2019Q2

Subject to Change

高性能VPN加速支持

SSL/TLS测试

专用硬件

ECC加密

高吞吐量

隧道建立

C100-S3/CF20专有硬件加速

全面支持HTTP/2和TLS 1.3

ECC加密性能40G以上

15万以上隧道建立速率

加速效果比较

硬件加速卡

密码族	吞吐量（Gbps）		
	硬件加速	无硬件加速	性能提升倍数
AES128-SHA256	40	7	5.71x
AES256-SHA256	40	6	6.66x
AES128-GCM-SHA256	40	13	3x
AES256-GCM-SHA384	40	10	4x
DHE-RSA-AES128-GCM-SHA256	40	12.5	3x
ECDHE-RSA-AES128-SHA256	40	6.9	5.8x
ECDHE-RSA-AES256-SHA384	40	6.9	5.8x
ECDHE-RSA-AES128-GCM-SHA256	40	12.5	3.2x
ECDHE-RSA-AES256-GCM-SHA384	40	10	4x
ECDHE-ECDSA-AES128-SHA256	40	7	5.67x
ECDHE-ECDSA-AES256-SHA384	40	6.9	5.7x
ECDHE-ECDSA-AES128-GCM-SHA256	40	12.6	3.2x
ECDHE-ECDSA-AES256-GCM-SHA384	40	10	4x

注意：上述性能基于8x10G， 512K Object size，16k record

产品优势汇总

- 高性能产品硬件C100-S3-MP
- 高性能加密加速卡
- 最高支持TLS 1.3协议测试
- 支持HTTP/2
- 支持业界领先的SAPEE
- 支持大规模数据库FormDB
- SAPEE 和FormDB打通
- 动态内容搜索和使用
- 10 个动作计时器
- 强大而精确的压力模型
- 内置网络真实性
- 支持PPTP协议
- 支持QUIC协议
- 支持Email over SSL
- 支持ABR over SSL
- 全面的运行时统计项
- 支持高达7天连续测试
- 内置SSL and IPSec 调试选项
- 支持DDOS和网络攻击
- 支持IPv4和IPv6双栈