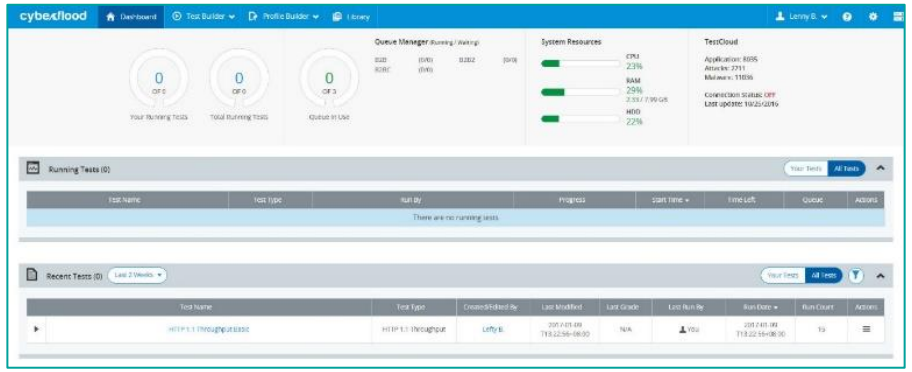
CyberFlood介绍

CyberFlood介绍

下一代应用和安全测试解决方案

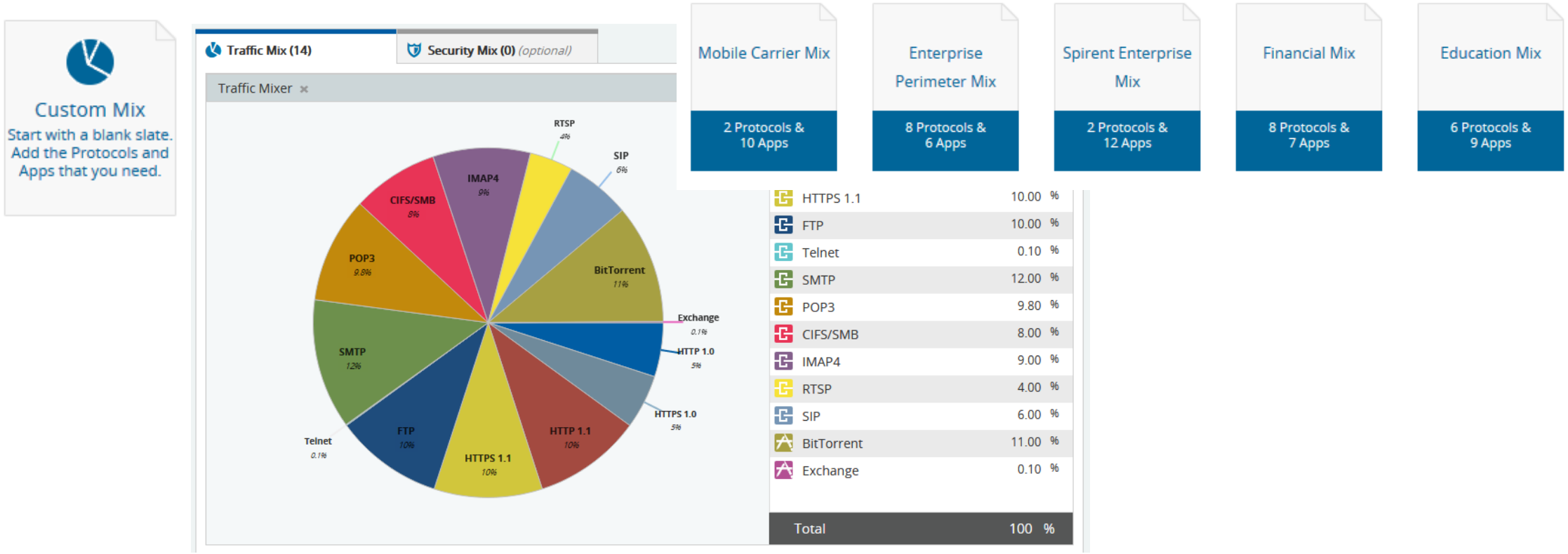
- 下一代应用与安全测试解决方案
- 多平台支持
  - C100-MP、C100-S3、CF20、C1
  - CyberFlood Virtual
  - 支持1G到100G接口
- 优势：
  - 大大提高易用性
  - 基于RFC的测试方法学：RFC 3511、NetSecOpen
  - 业内唯一全面支持安全测试的解决方案：DDoS、已知攻击、Malware、Fuzzing
  - 大PCAP文件回放 – 最大支持10GB文件
  - 通过地图选择子网
  - 支持10，000多种真实业务场景
  - 支持多种流媒体视频测试
  - 支持20,000多种攻击和恶意软件



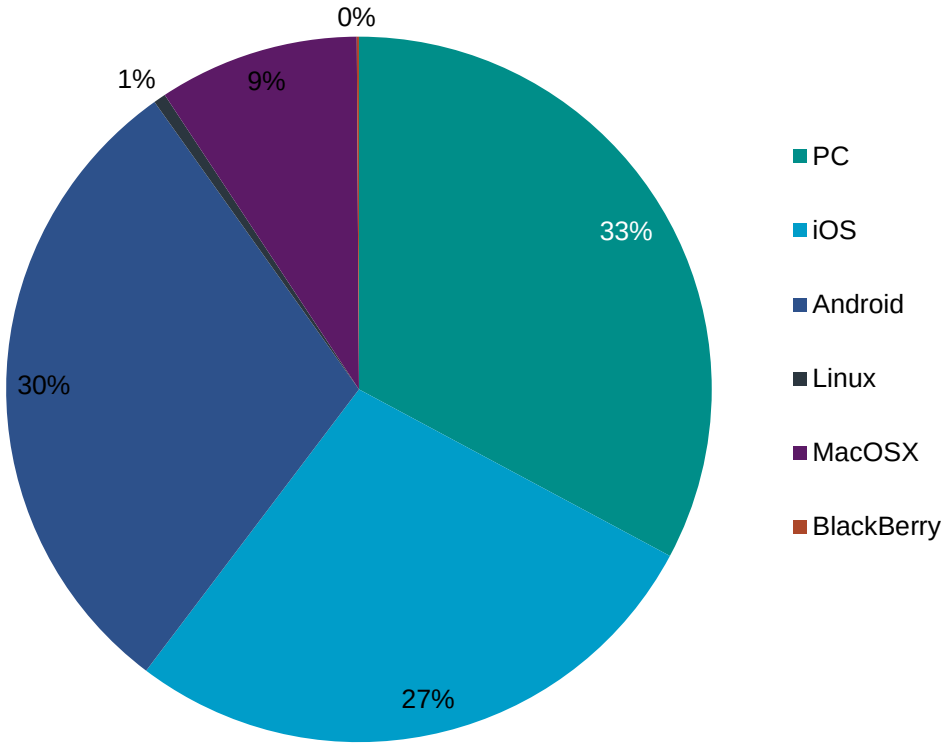
CyberFlood混合应用测试

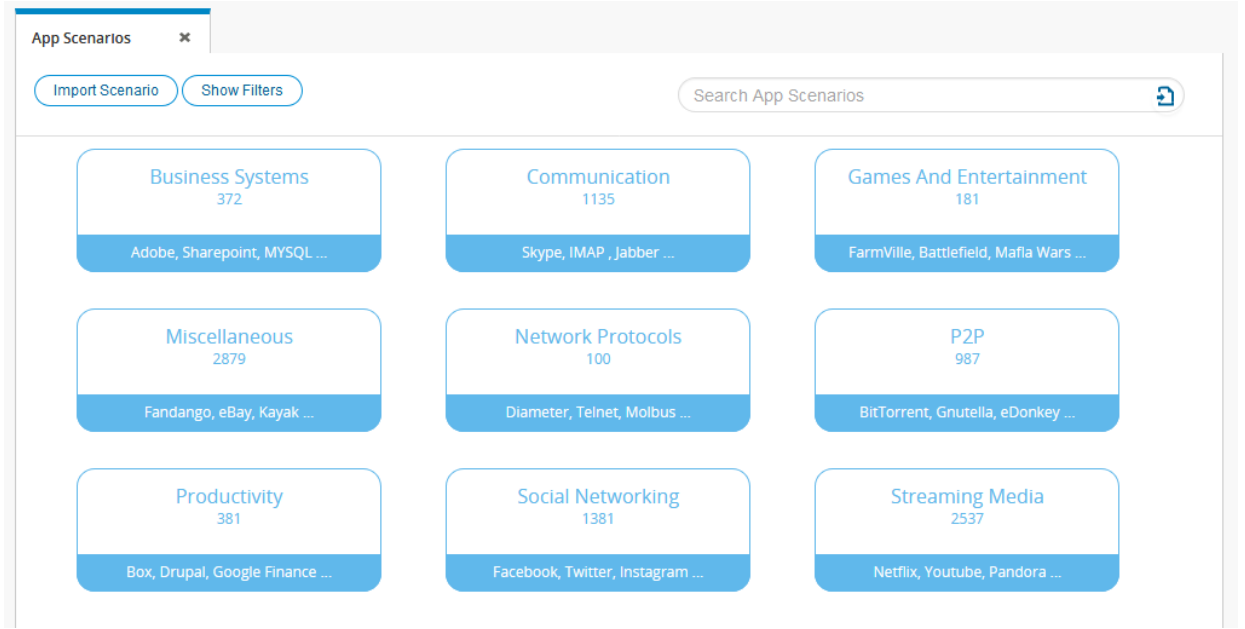
支持混合应用测试，多种内置模板

- Mix any app from TestCloud Samples
- Add your own test scenario via har or pcap



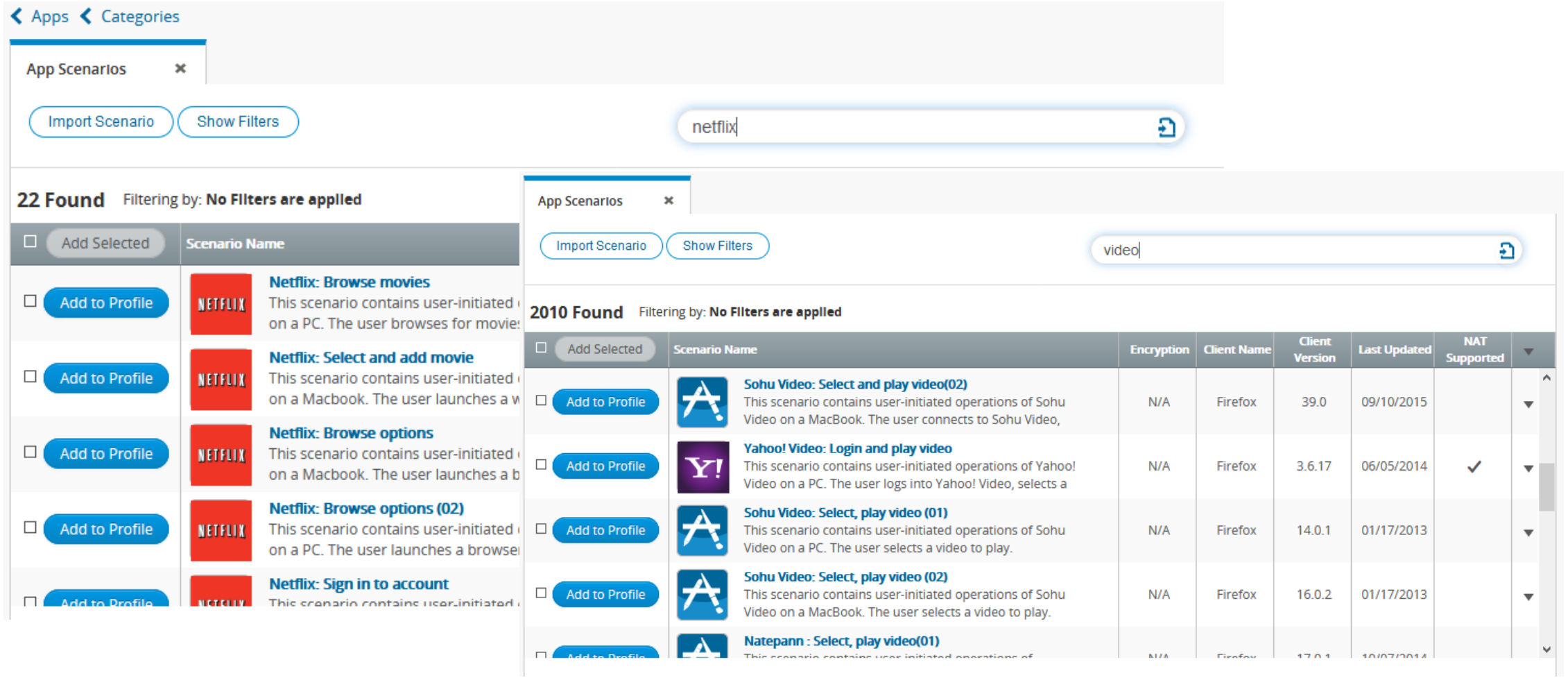
Cyberflood – 10000+ 应用分布





CyberFlood场景

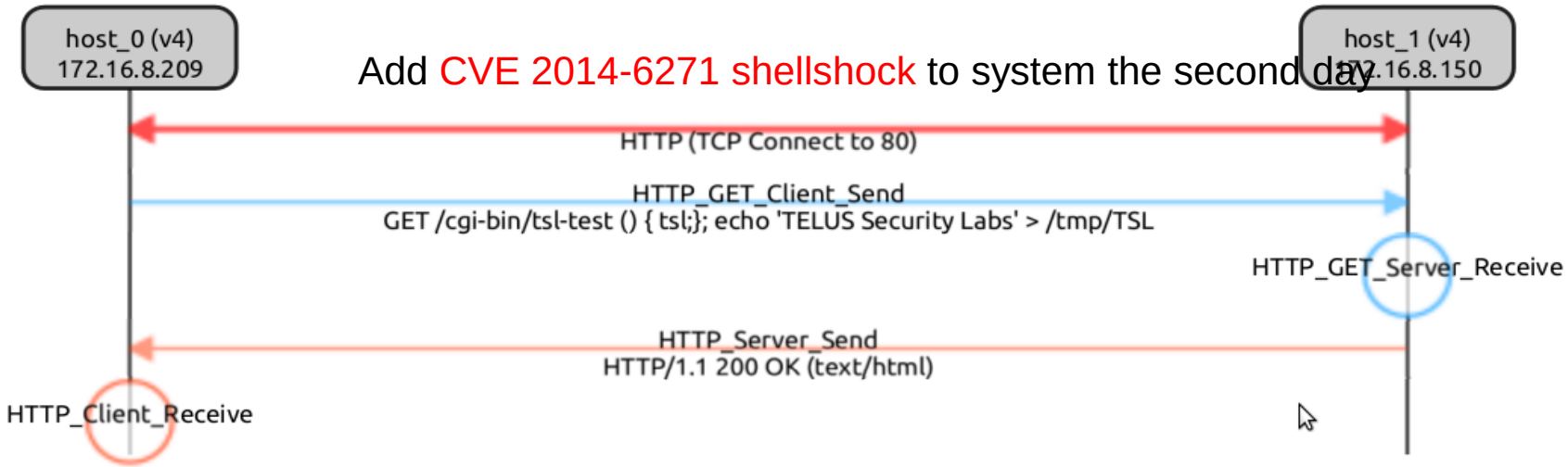
Netflix和多种视频



CyberFlood 攻击

CVE 2014-6271 破壳漏洞攻击

A command execution vulnerability exists in GNU Bash. The vulnerability is due to a failure in handling environment variables. A remote attacker can exploit this vulnerability by interacting with an application that uses Bash environment variables. If an attacker can control the value of an environment variable, then command execution can be achieved in the context of the application using the environment variable.



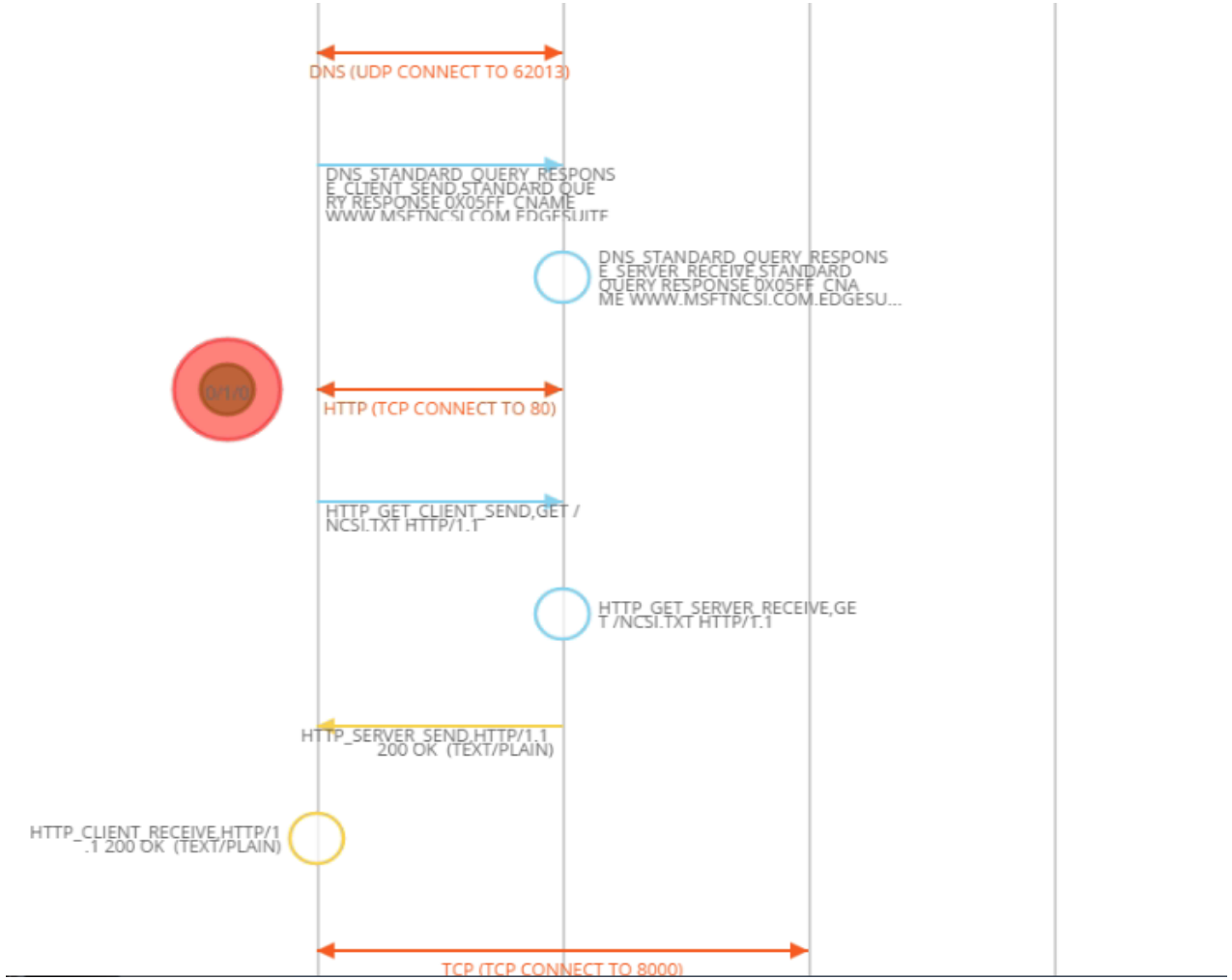
SNORT

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"OS-OTHER Bash CGI environment variable injection attempt"; flow:to_server,established; content:"() {"; fast_pattern:only; http_header; metadata:policy balanced-ips drop, policy max-detect-ips drop, policy security-ips drop, ruleset community, service http; reference:cve,2014-6271; reference:cve,2014-6277; reference:cve,2014-6278; reference:cve,2014-7169; classtype:attempted-admin; sid:31978; rev:5;)

CyberFlood 攻击

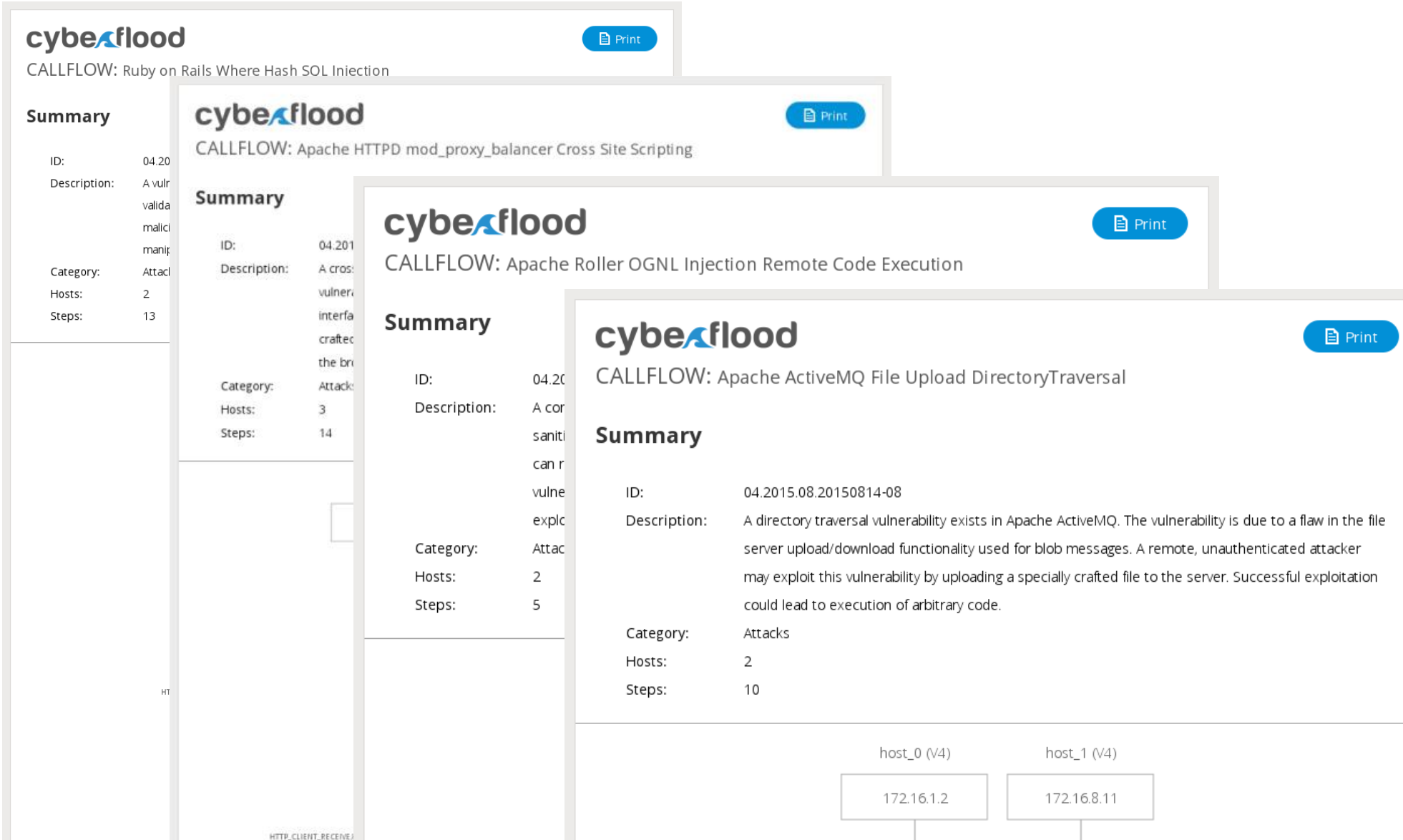
显示那个步骤被拦截

- 测试攻击和恶意软件时，DUT拦截内容并触发告警
- 拦截的位置至关重要
- 是否正确拦截并触发告警？是否拦截错误了？
- 例子显示DNS流量放行，HTTP流量被拦截。



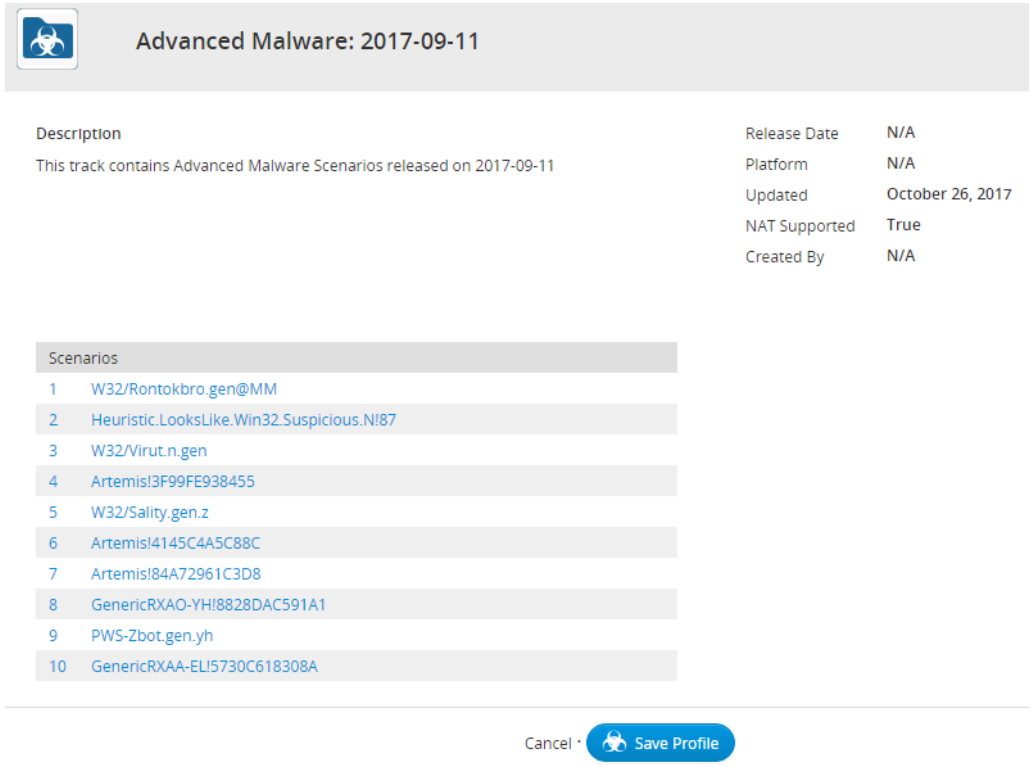
支持多种攻击类型

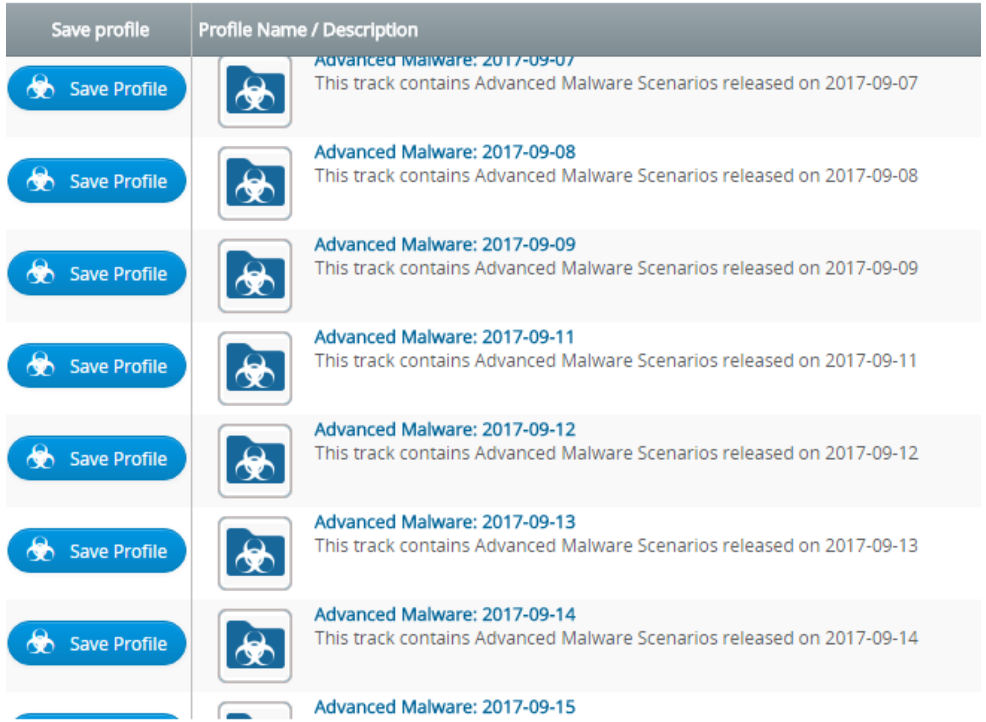
- SQL注入
- XSS跨站共计
- 远程代码执行
- 目录遍历
- 释放后重用
- 应用层攻击



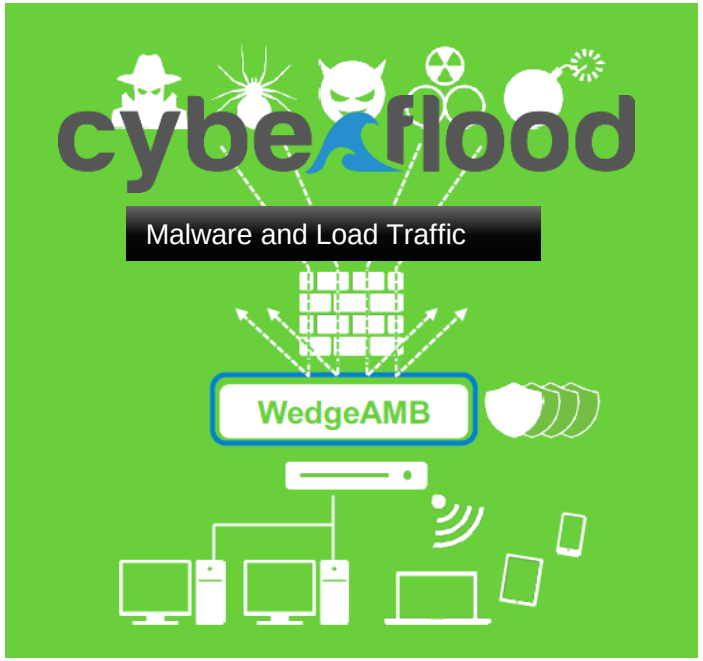
高级恶意软件每天数次更新

- Multiple update each day
- 总数超过17000种



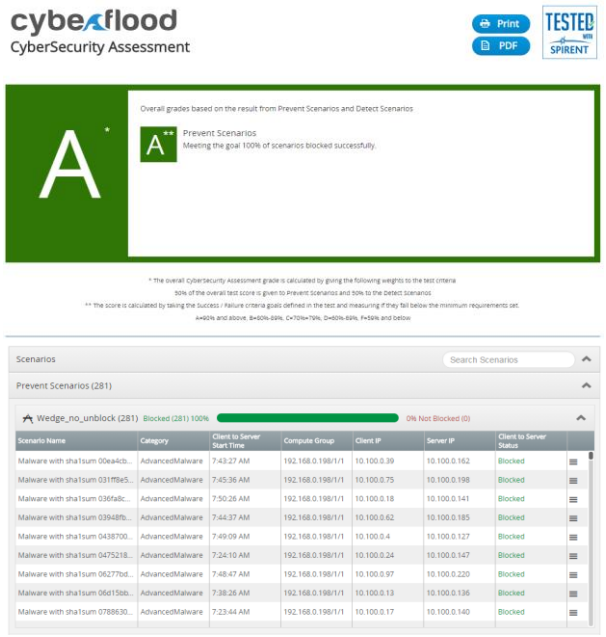


案例 - WedgeAMB 恶意软件防御

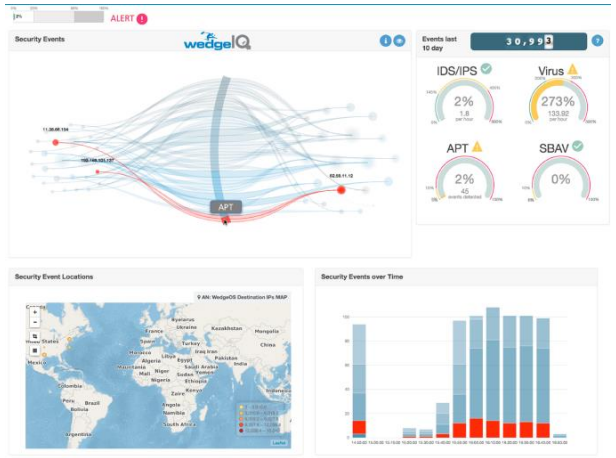


Wedge Advanced Malware Blocker (WedgeAMB)

- Orchestrates Signature, Heuristic, and AI AV technologies to block known and unknown malware in real-time
- Delivers the accuracy of a Sandbox with the latency and in-line blocking performance of an IPS



CyberFlood targeted WedgeAMB with both known and unknown malware samples – including command and control traffic

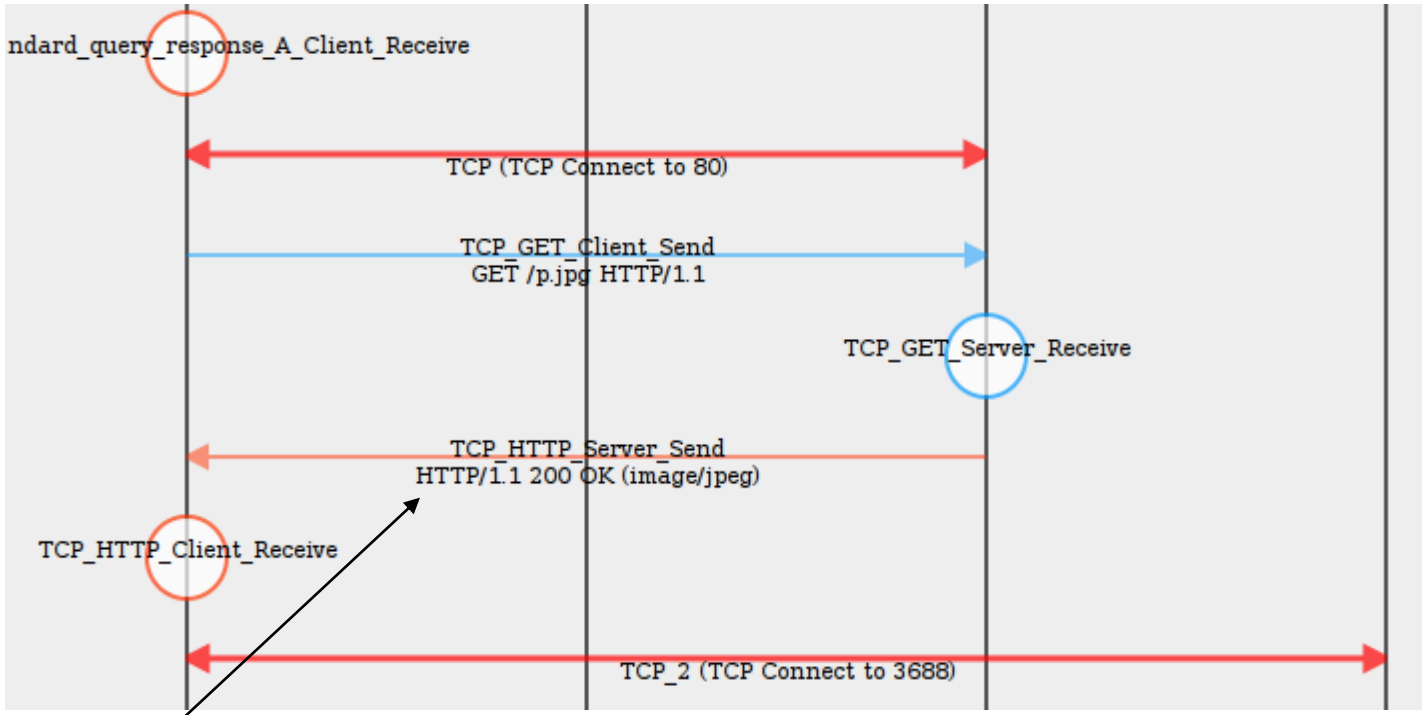


WedgeAMB showcased attack blocking capabilities and performance

CyberFlood Botnet恶意软件

恶意软件行为分析

```
# HTTP/1.1 200 OK  (image/jpeg)
      TCP_HTTP_Server_Send = TCP.server_send {
         struct [
            "HTTP/1.1 200 OK\r\n"
            "X-MU-Session-ID: #{@tcp_sid}\r\n"
            "Date: Mon, 28 Sep 2009 17:45:54 GMT\r\n"
            header(header_name: "Content-Length") [
               length_string(of: content_1)
            ]
            "Content-Type: image/jpeg\r\n"
            "Content-Location: http://back.mm972.com/p.jpg\r\n"
            "Last-Modified: Sat, 22 Aug 2009 06:15:19 GMT\r\n"
            "Accept-Ranges: bytes\r\n"
            "ETag: \"bec24fecef22ca1:76c8d\"\r\n"
            "Server: Microsoft-IIS/6.0\r\n"
            "X-Powered-By: ASP.NET\r\n"
            "\r\n"
              content_1 = "[61.164.108.99:3688]"
         ]
      }
```

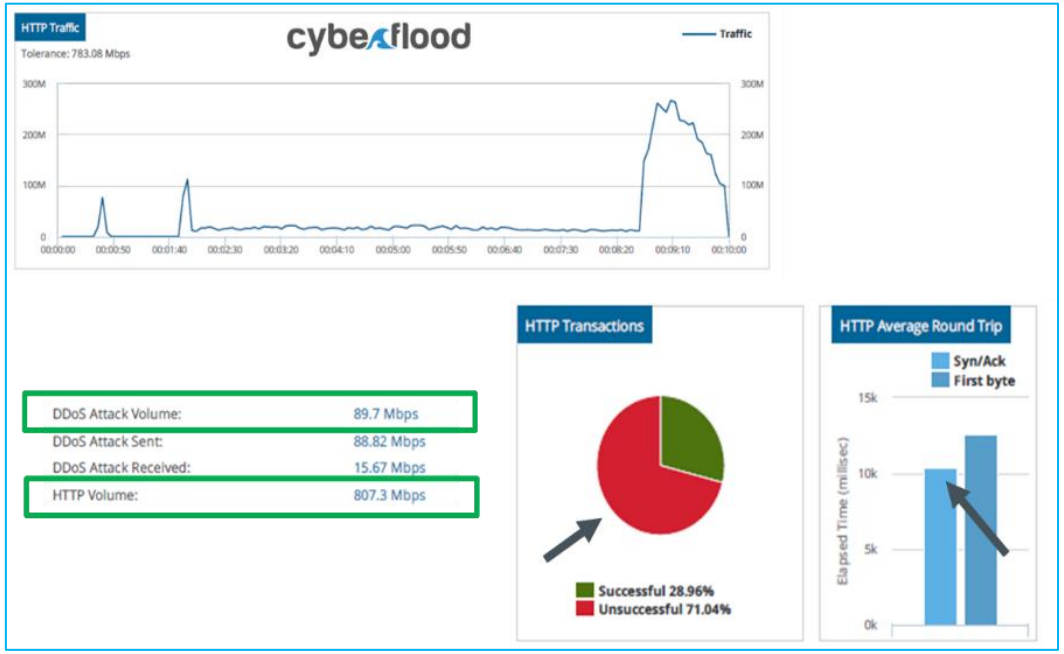


- Add new activity
- Modify contents
- Training
- Study botnet communication and hidden method

CyberFlood DDoS测试

验证抗D设备性能

- 线速DDoS 攻击(多个10G接口)
- 长时间DDoS攻击
- 混合攻击 (合法HTTP 流量 + DDoS 攻击)
- 纯攻击模式
- 单臂DDOS攻击



这些报文会导致服务崩溃吗

- Standard HTTP GET request
  - GET /index.html HTTP/1.1
- Fuzzing is a technique used by Development and QA teams to find Zero-Day vulnerabilities
  - AAAAAA...AAAA /index.html HTTP/1.1
  - GET ///////index.html HTTP/1.1
  - GET %n%n%n%n%n%n.html HTTP/1.1
  - GET /AAAAAAAAAAAAA.html HTTP/1.1
  - GET /index.html HTTTTTTTTTTTTTP/1.1
  - GET /index.html HTTP/1.1.1.1.1.1.1.1

- Fuzzers can inject null characters, numeric values, and quotes to cause buffer overflows and other undesired behavior

当前支持Fuzzing协议

Groups	Protocols									
Authentication (AAA)	802.1X	DIAMETER	LDAP	RADIUS						
Encryption	GRE	IKEv1	IKEv2	SSHv1	SSHv2					
IPv4	DHCPv4	ICMPv4	IPv4	TCPv4	UDPv4					
IPv6	ICMPv6	IPv6	MLD	NDP	TCPv6	UDPv6				
IoT	MQTT									
Link Layer	PPP	PPPoE								
Mail Services	IMAP4	POP3	SMTP							
Mobility	GTPv1	GTPv2								
Multimedia	RTP	RTSP	SIP							
Network Configuration	SNMP TRAP	SNMPv1	SNMPv3							
Network Discovery	ARP	DHCPv6	IGMPv3	LLDP						
Network Services	DNS	FTP	NTP	TELNET	TFTP					
Routing 1	BGPv4	DVMRP	IS-IS	MPLS	PIM-SM IPv4	PIM-SM IPv6	PIM-SSM IPv4	PIM-SSM IPv6	VRRPv2	VRRPv3
Routing 2	OSPFv2	OSPFv3	RIPng	RIPv2						
SCADA	DNP3	GOOSE	IEC104	IEC61850	MMS	MODBUS	PROFINET-DCP			
Switching	802.1Q	VxLAN	RTSP	STP	MSTP					
Web Services	HTTP	HTTP/2	SSL/TLS	TLS1.2	TLS1.3					
Total	74									

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

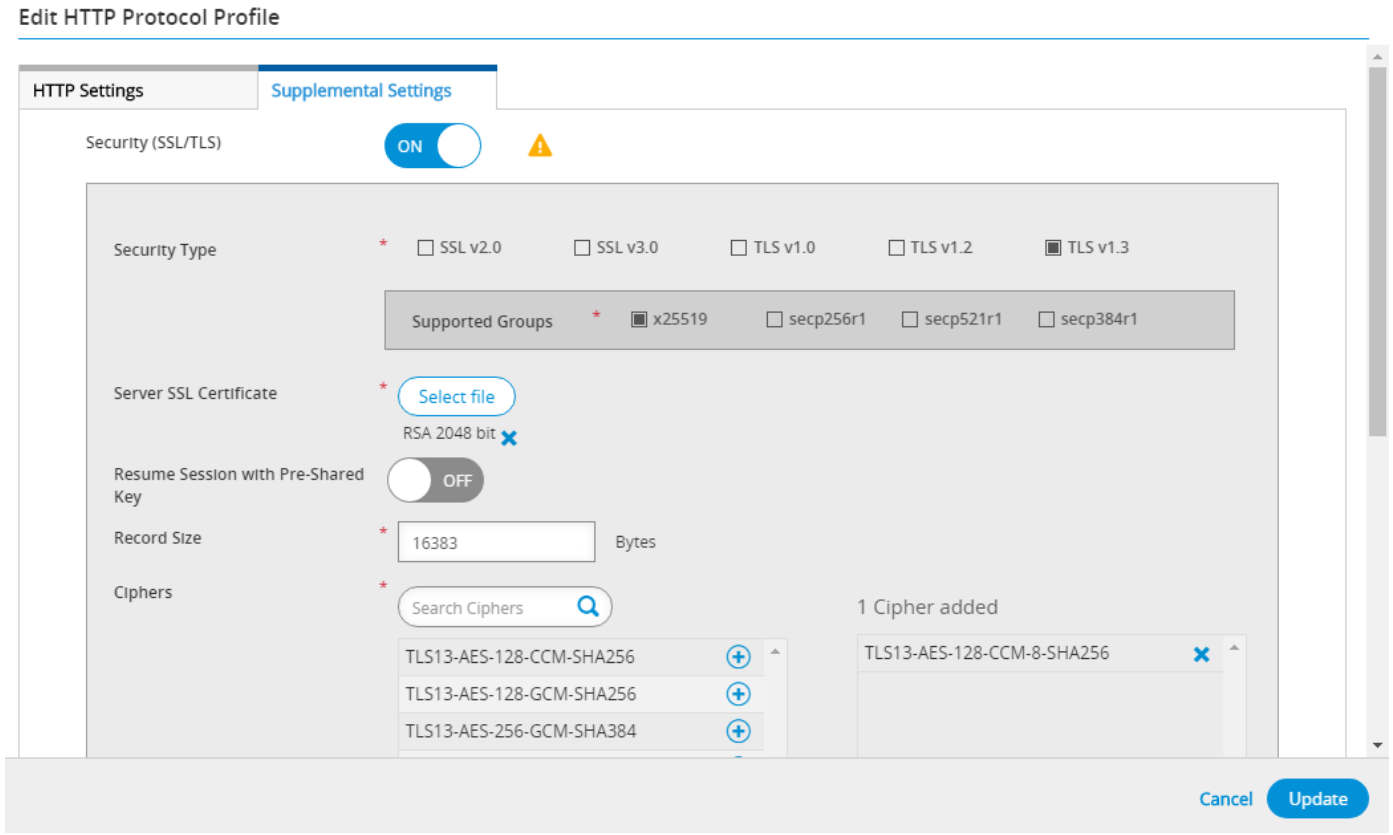
硬件加速卡

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

TLS v1.3

- **第一时间支持**
  - 模糊测试
  - 性能测试
- 支持RFC正式版本



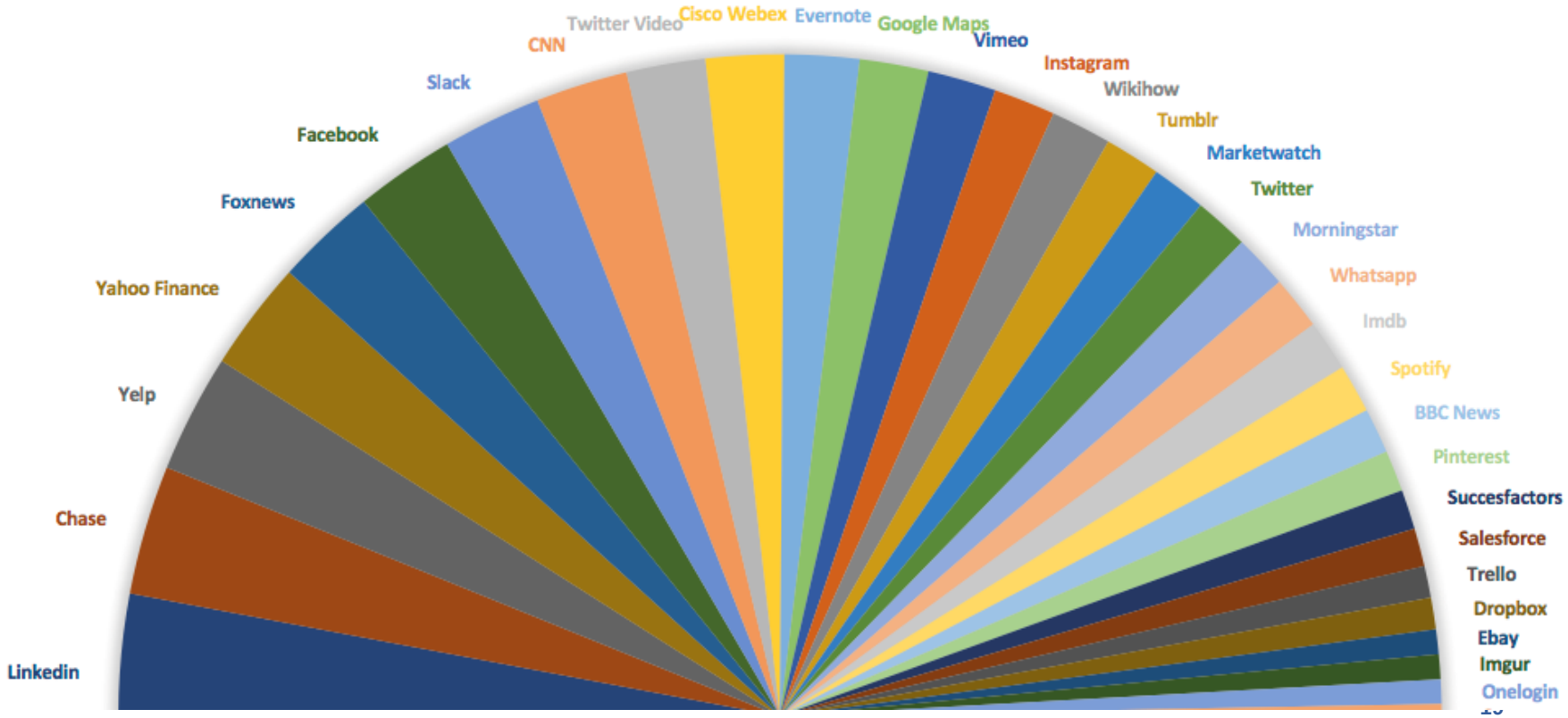
网络安全测试标准

封闭标准 → 开放标准

厂商私有标准

NetSecOPEN 测试联盟

- 最新的公开和全面的NGFW 流量模型，支持防火墙，IPS和下一代防火墙测试
- https://tools.ietf.org/html/draft-balarajah-bmwg-ngfw-performance-04
- 混合 ~70% HTTPS 和~30% HTTP
- ~10K 独立网址
- ~1000 个 域名
- ~400 个不同的证书
- ~80 种应用



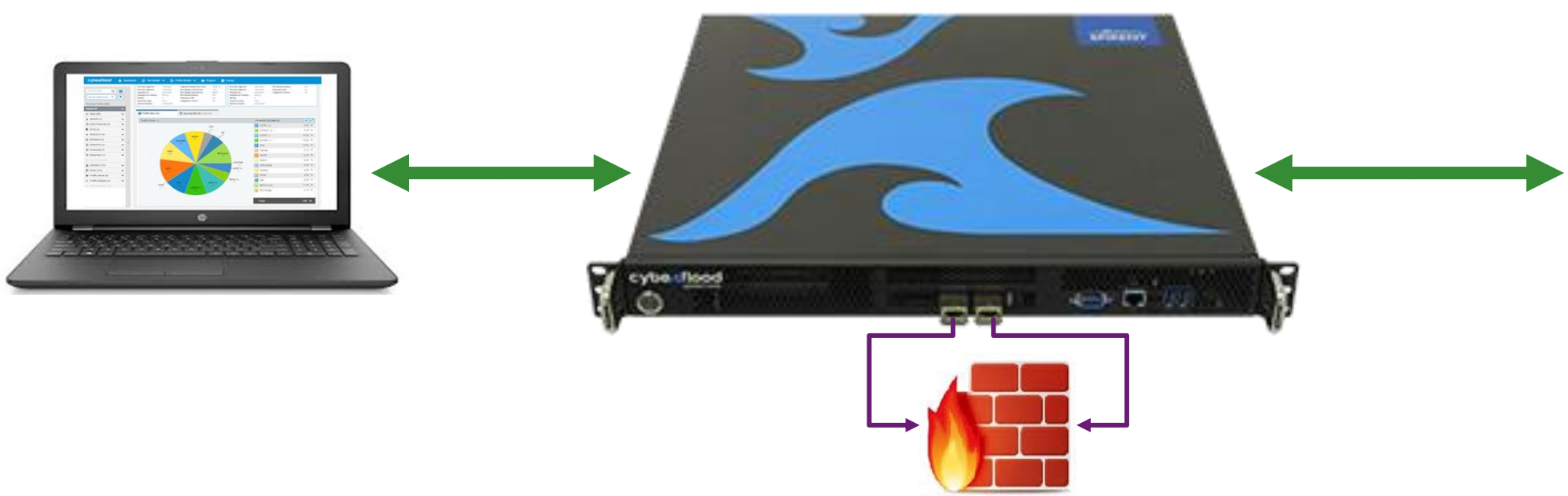
2018平台一览

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**

CF20使用三部曲



被测设备

1. 打开浏览器，输入 CF20 地址

2. 开始测试

3. 获取测试结果

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

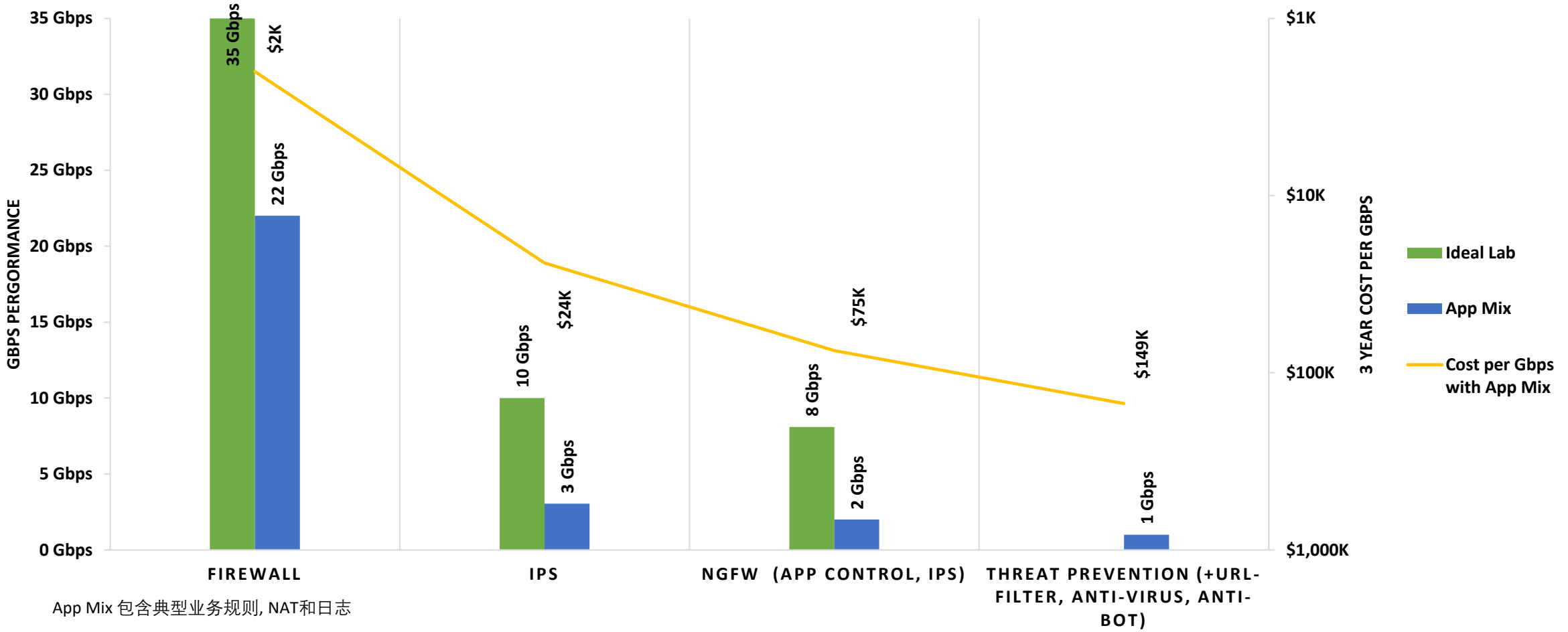
- 性能（每对虚拟端口）
  - 5倍于Avalanche Virtual：10Gbps，50万并发，5万新建
- 目前支持平台
  - VMware ESXi (5.5, 6.0, 6.5)
  - KVM (Ubuntu 16.04 LTS tested)
- 软件支持
  - CyberFlood
  - Avalanche
- 支持云平台
  - Amazon AWS 2018Q4支持
  - OpenStack → 2019Q1
  - Microsoft Azure → 2019Q2

Subject to Change

性能数据：理想与现实的差距

二代防火墙测试

同一台二代防火墙，开启不同的功能，测试出性能和每Gbps的价格

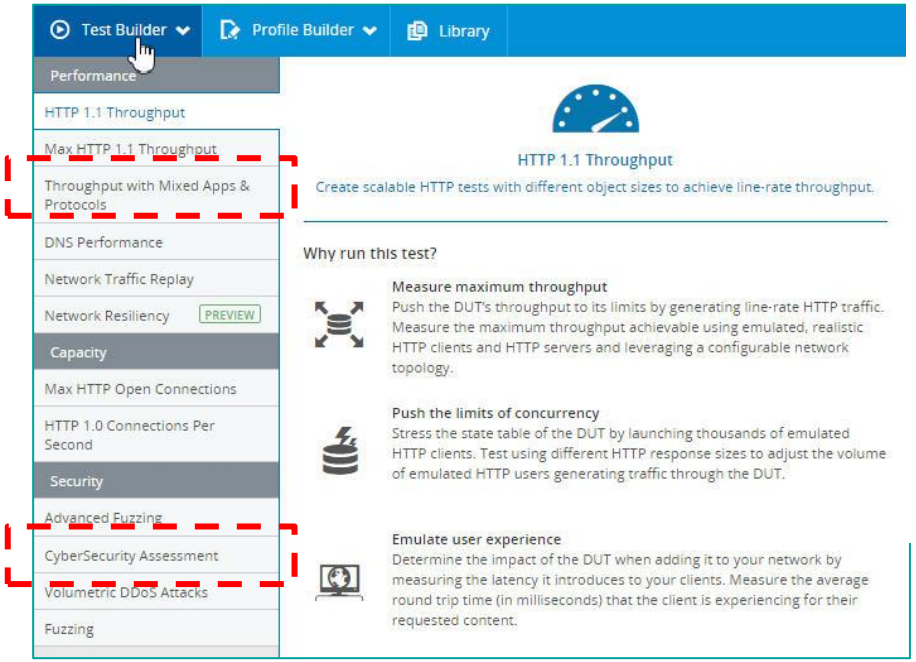


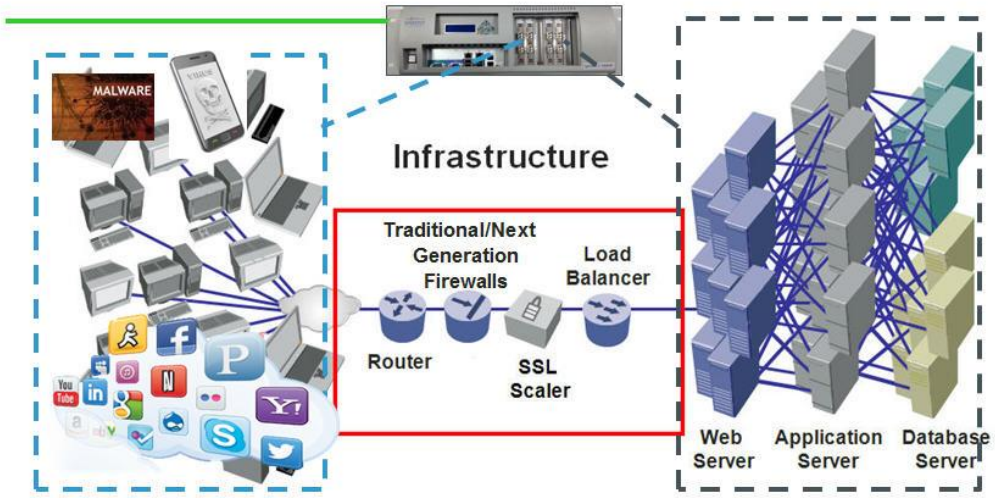
App Mix 包含典型业务规则, NAT和日志

数据来源: 业界领先的NGFW厂商的一组公开测试数据

CyberFlood 系统

网络/安全/应用性能测试

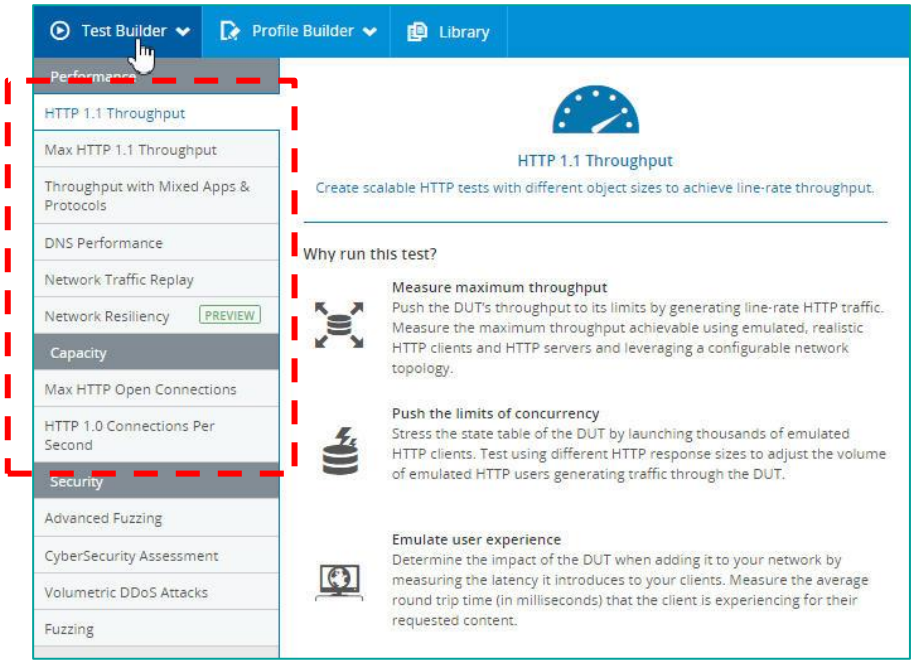


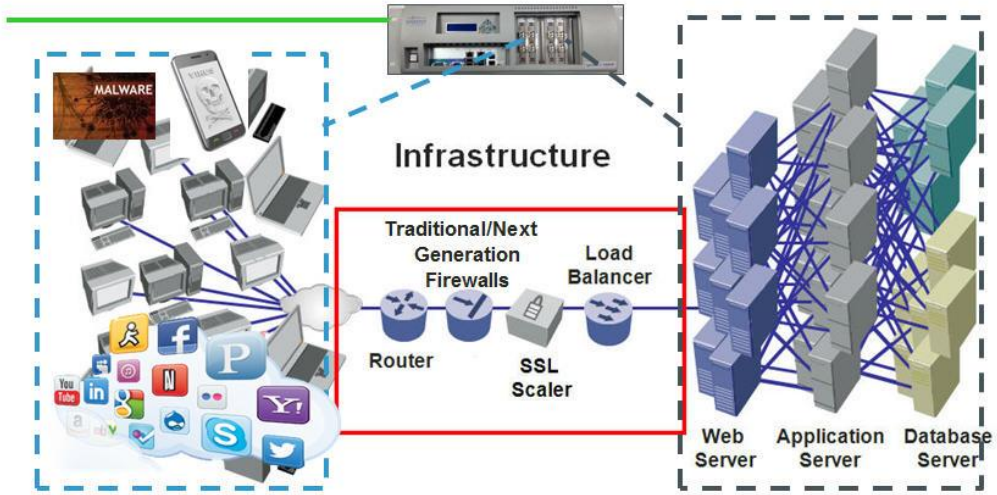


主要测试领域	亮 点
• 验证网络安全和互联网性能测试 • 在真实流量背景下验证攻击和恶意软件拦截能力	• 混合应用和攻击验证网络设施 • 加载3500多种攻击样本 • 上万种真是的局域网和互联网业务场景 • 模拟真实恶意软件行为

CyberFlood 系统

协议性能测试

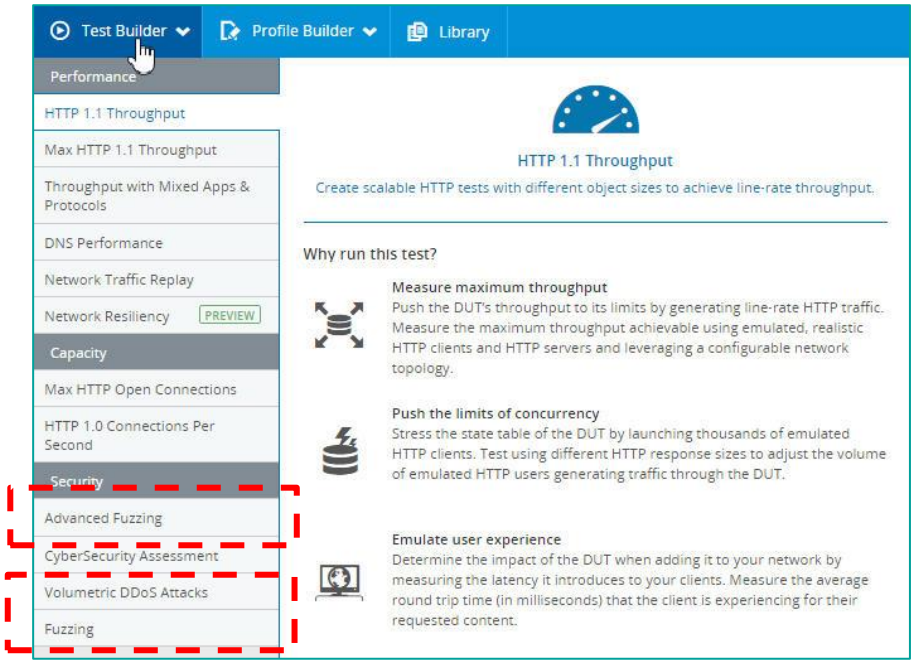


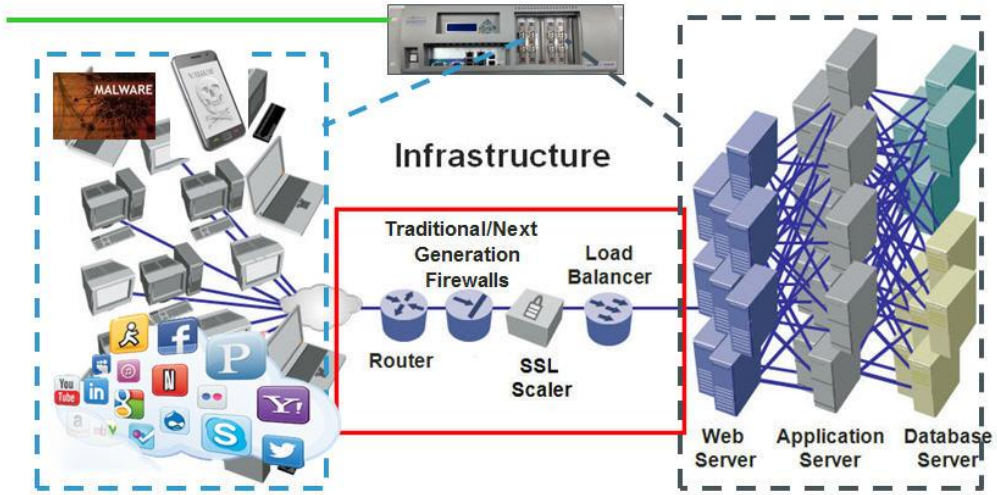


主要测试领域	• 4层设备网络性能测试
亮 点	• 产生线速的流量 • 产生真实网络混合业务场景 • 高达数百万的TCP新建和数千万的网络并发

CyberFlood 系统

模糊测试/DDoS测试





主要测试领域	亮 点
• 通过模糊测试和**DDoS**测试验证设备，主机和网络的稳定性。 • 用**Fuzzing**对多种协议做模糊测试	• 找出产品缺陷，避免潜在的**0**日漏洞 • 快速重现问题

CyberFlood 系统

应用/系统测试

- 通过Avalanche Commander配置进行复杂的应用和系统测试。