



下一代网络安全测试方法



曲博

Bo.Qu@Spirent.Com

测试，能给网络安全带来什么？

- ◉ 网络安全设备性能评估
- ◉ 网络安全设备对攻击的识别和阻断能力评估
- ◉ 网络安全设备选型和入网评估
- ◉ 在网络部署之前，评估承载和安全能力
- ◉ 安全测评体系的支持
- ◉ 赛博靶场（Cyber Range）
- ◉ 网络安全竞赛
- ◉ 网络安全培训

测试，对于网络安全的重要性

- 如何保证网络或设备的性能和安全性？
- 如何平衡性能和安全性？
- 如何保证正确处理最新的应用/内容？
- 如何保证网络或设备在处理真实流量时，保持性能和安全性？



最早与安全设备相关的性能测试标准RFC 3511

测试项目	测试指标注释	网络分层	关键性
IP Throughput	吞吐量	L2-3	No
Concurrent TCP Connection Capacity	最大并发TCP连接数	L4-7	Yes
Maximum TCP Establishment Rate	最大TCP连接建立速率 (CPS)	L4-7	Yes
Maximum TCP Teardown Rate	最大TCP连接拆除速率	L4-7	No
Denial of Service Handling	拒绝服务攻击处理能力	安全性	No
HTTP Transfer Rate	HTTP有效吞吐量 (Goodput)	L4-7	Yes
Maximum HTTP Transaction Rate	最大HTTP事务处理速率 (TPS)	L4-7	Yes
Illegal Traffic Handling	非法数据流处理	安全性	No
IP Fragmentation Handling	IP分片处理	安全性	No
Latency	延迟	L2-3	No

思博伦是防火墙测试国际标准的主要制定者

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.

Copyright Notice

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



防火墙测试新条目 – 国内某运营商

测试项目	测试目标	网络分层
并发连接测试 (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： <ul style="list-style-type: none">• 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，如“新浪”• 验证重叠、乱序包能正确处理	L4-7
新建连接测试 (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
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
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
IPSec测试	测试防火墙IPSec容量，IPSec新建速率，IPSec流量	L3-7
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

互联网应用爆炸性增长



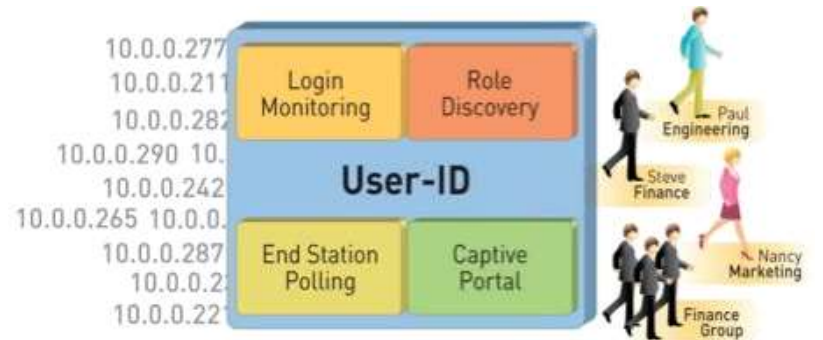
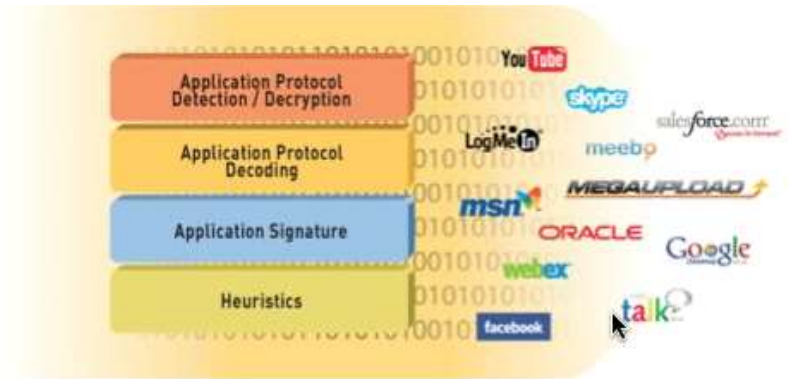
各种复杂应用模拟测试方法

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，如果需要，则下载更新 – TestCloud数据库
- 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 (PCAP导入)



SPIRENT

经常更新的应用库TestCloud/Store

AvalancheNEXT Store

QQ

Business Systems

Adobe, Sharepoint, MYSQL

Miscellaneous

Fandango, eBay, Kayak

Productivity

Box, Drupal, Google Finance

Communication

Skype, IMAP, Jabber

Network Protocols

Diameter, Telnet, Modbus

Social Networking

Facebook, Twitter, Orkut

Games and Entertainment

Farmville, Battlefield, Mafia Wars


P2P

BitTorrent, Gnutella, eDonkey


Streaming Media

Netflix, YouTube, Pandora


Featured Tracks




Travel




Online Gaming




Netflix



iTunes




Internet Radio




2Shared


New Tracks




AppID: P2P




Skype Voice Ca...




Google Tools



Enterprise Appli...



Spirent: Skype



Voice Calls


Top Searches

1. Netflix
2. Silverlight
3. Google
4. Skype
5. Facebook
6. Yahoo!
7. Twitter
8. Sharepoint
9. Ryze
10. AIM

9

PROPRIETARY AND CONFIDENTIAL - Not for Dissemination without Spirent's written consent.

All Dates are Subject to Change Without Notice



SAPEE Editor

File Edit Help

Client IP: 192.168.1.69 Server IP: 207.46.106.101 Close: Client/FIN Transport: TCP

Pkt #	Direction	Time(ms)	Delay(ms)	Data
1	→	0	0	VER 4 MSNP15 M...
2	←	97	97	VER 4 MSNP15..
3	→	97	0	CVR 5 0x0409 wi...
4	←	197	100	CVR 5 8.1.0178 ...
5	←	200	3	GCF 0 6519..<Po...
6	←	202	2	pcA==" /> <!--
7	←	309	107	ZhbnNclmluZm8...
8	←	310	1	g4LWpwZ1wueml...
9	←	312	2	text value="Y2gz...
10	←	409	97	m9iem9wXC5jb20...
11	→	973	564	USR 7 SSO S t=E...
12	←	1124	151	USR 7 OK shekha...
13	←	1124	0	SBS 0 null..
14	←	1128	4	MSG Hotmail Hot...
15	←	1128	0	nabled: 0....
16	→	1285	157	BLP 8 BL..
17	→	1308	23	ADL 9 2866..<ml ...
18	→	1308	0	c n="taurus_tan...
19	→	1308	0	c n="beverlyriwa...
20	←	1378	70	BLP 8 BL..

Insert Packet
Cut Packet
Copy Packet
Paste Packet
Delete
Move Up
Move Down
Reverse Packet
Verify
Search
Add Loop...
Add Timer...

Insert Variable
Define Variable...

ASCII Editor

```

text
value="Y2gzY2szclwu
aW5mbw==" />
<imtext
value="cjU3OWRrYTky
alwuemlw" />
<imtext
value="MjAzXC4xNTVc
  
```

#	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E
0	74	65	78	74	20	76	61	6c	75	65	3d	22	59	32	6'
10	59	32	73	7a	63	6c	77	75	61	57	35	6d	62	77	3
20	22	20	2f	3e	20	20	20	20	20	20	3c	69	6d	74	6'
30	74	20	76	61	6c	75	65	3d	22	63	6a	55	33	4f	5'
40	72	59	54	6b	79	61	6c	77	75	65	6d	6c	77	22	2i
50	3e	20	20	20	20	20	20	3c	69	6d	74	65	78	74	2i
60	61	6c	75	65	3d	22	4d	6a	41	7a	58	43	34	78	4
70	56	63	4c	6a	63	30	58	43	34	35	4d	53	39	6c	6i
80	6c	69	4c	32	4a	73	62	32	63	76	59	6d	78	76	5
90	77	75	61	48	52	74	62	41	3d	3d	22	20	2f	3e	2i

构造复杂的应用场景性能测试

The image displays the Spirent TestCloud interface, which is used for configuring and executing performance tests. It is divided into several main sections:

- Library (Left Panel):** A sidebar containing a list of application categories and specific test tracks. The 'AppID: Games' category is currently selected.
- Store / Player / Library (Middle Panel):** A central area for managing test assets. It shows a 'View: All Users' Tracks' dropdown and a list of available tracks, including '1111', '2Shared', 'All Attack', and various 'AppID' categories.
- Select a Test Template (Right Panel):** A section for choosing a test template. Three templates are visible:
 - CyberSecurity Assessment:** Run over ten thousand modern and advanced instances of attacks and malware.
 - Application Identification:** Create high volumes of the latest mobile and cloud applications, as well as security traffic patterns.
 - Reliability Testing:** Perform long-duration tests with the full Spirent TestCloud application load.
- Test Configuration (Bottom Panel):** A detailed view of a test configuration for 'Untitled-Test-21'. It includes:
 - Duration:** Set to 00:01:00.
 - Play through NAT:** A checkbox option.
 - Track Mixer:** A visual representation of the test traffic composition, showing a mix of different application types (represented by colored bars) and their relative proportions (e.g., 10%, 10%).
 - Loaded Tracks (8):** A list of the specific application tracks loaded for the test.
 - Test Queue:** A section for configuring the test queue, showing 'Alpha' and 'SPT-C100-MP-3'.
 - Measurement:** A section for selecting the measurement type, currently set to 'Bandwidth'.

网络安全攻击现状

- **恶意软件**（病毒、蠕虫、木马、宏病毒、垃圾邮件、间谍软件、广告软件、Rootkit、记键程序，等等），Botnet、网络入侵、DDoS攻击、网络钓鱼、数据窃取， ...



- 针对新互联网应用的新变种（社交网络）
- <http://www.f-secure.com/weblog/archives/00001517.html> (Facebook)
- <http://thenextweb.com/twitter/2013/04/22/criminals-hijack-twitter-accounts-using-malware-that-injects-javascript-code-to-send-malicious-tweets/> (Twitter)

DDoS仿真测试方法

大流量DDoS仿真测试

- 源自长期安全研究积累、借助硬件流量发送能力
- 开放接口，用户可以自行构造添加新的DDoS攻击
- 多种流量模型（ Ramp、Burst、Random、Pulse ）
- 检测正常业务是否被阻断

DDoS 和正常流量混合

- 混合DDoS 流量和正常流量
- 衡量正常流量用户体验，衡量DDoS流量阻断效果
- 测试设备CPU占用率和队列深度

内嵌攻击

- 用特有的动作列表和模拟用户技术来模拟中间人攻击
- 在IPSec VPN和SSL VPN隧道上产生攻击



已知攻击/漏洞测试方法

- 支持8000多种攻击手法
- 攻击库每月更新
- 攻击模型包含了多种软件平台和攻击场景
- 混合攻击流量和业务背景流量使用同一个端口发送
- 同时测试恶意攻击识别能力和系统的正常业务处理能力

Malware: 2014-07	
	name
	Malware: 2014-07
Attacks: 2014-07	
	name
	Attacks: 2014-07
	Attacks: 2014-07
	name
13.	Symantec Web Gateway dbutils.php SQL Injection
14.	Samba nmbd sys_recvfrom Infinite Loop Denial of Service
15.	Oracle Event Processing FileUploadServlet Directory Traversal
16.	Microsoft Internet Explorer CVE-2014-2804 Use After Free
17.	Microsoft Internet Explorer CVE-2014-1765 Use After Free
18.	AlienVault OSSIM av-centered Util.pm Request Arbitrary Command E
19.	D-Link HMAP Request Stack Buffer Overflow
20.	HP Intelligent Management Center BIMS UploadServlet Information
21.	HP Intelligent Management Center SyslogDownloadServlet Informat
22.	Oracle Business Intelligence Mobile App Designer Information Disc
23.	Oracle Java AtomicReferenceFieldUpdater Type Confusion
24.	HP Data Protector Opcode 28 and 11 Command Execution
25.	Oracle Database Server LpxFSMSax QName Stack Buffer Overflow

OpenSSL心脏滴血攻击流程展示

- 通过图形化交互流程，形象地展示攻击流程
- 把攻击报文转换成开放的过程描述语言MSL，便于专业人士理解修改

```
# Server Hello
TLsv1_1_Server_Hello_Client_Receive = TLsv1_1_Server_Hello_Server_Send.client_receive

# Continuation Data
TLsv1_1_Continuation_Data_Client_Send = TLsv1_1.client_send {
  0h188382008301ffff
}

# Continuation Data
TLsv1_1_Continuation_Data_Server_Receive = TLsv1_1_Continuation_Data_Client_Send.server_receive

# Certificate, Server Hello Done, Continuation Data
TLsv1_1_Certificate_Server_Send = TLsv1_1.server_send {
  # record|TLSv1.1 Record Layer: Handshake Protocol: Certificate
  struct [
    # record_content_type|Content Type: Handshake (22)
    22:8
    # record_version|Version: TLS 1.1 (0x0302)
    0x0302:16
    # record_length|Length: 614
    614:16
    # handshake|Handshake Protocol: Certificate
    struct [
      # handshake_type|Handshake Type: Certificate (11)
      11:1
    ]
  ]
}
```

Callflow of [OpenSSL TLS DTLS Heartbeat Information Disclosure]

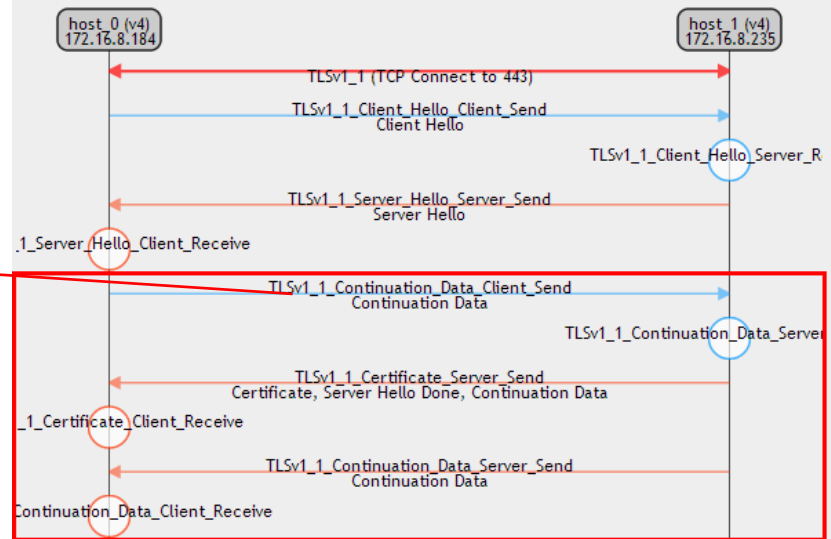
ID: 04.2014.04.20140408-01

Description: An information disclosure vulnerability exists in OpenSSL. The vulnerability is due to an error when handling TLS/DTLS heartbeat packets. An attacker can leverage this vulnerability to disclose memory contents of a connected client or server.

Category: Attacks

Hosts: 2

Steps: 11



用纯脚本编写攻击和应用场景

- 提供描述两个主机之间多种协议交互的纯文本场景语言MSL
- 所有系统内置的攻击都可以导出MSL脚本
- 可以描述从2层到7层的简单和复杂场景
- 用户只需描述关键部分
- 用户可以根据现有攻击和漏洞，编写新的攻击变种
- 编写私有0day漏洞，通过测试仪器检验赛博靶场（Cyber Range）效果

Tests

Results

Tracks

Scenarios

All 1730 Scenarios

Applications

Attacks

Malware

Upload Scenario

Actions

	name	severity	date	cve	secu...	bugt...	
	3vix MPEG-4 MP4 File Handling Stack Overflow	HIGH	12/10/2...		27998	26773	
	3S Smart Software Solutions CoDeSys Gatew...	CRITICAL	4/17/2013	2012-4...	52253		
	3S Smart Software Solutions CoDeSys Gatew...	CRITICAL	4/24/2013	2012-4...	52253		
	3S Smart Software Solutions CoDeSys Gatew...	CRITICAL	4/19/2013	2012-4...	52253		
	7T Interactive Graphical SCADA System File ...	CRITICAL	4/1/2011	2011-1...			
	ABB Multiple Products RobNetScanHost.exe ...	HIGH	3/9/2012	2012-0...	48090		

Delete
Download MSL
Download PCAP
View Callflow

```
scenario |
    scenario {
        hosts {
            # 172.16.8.21]
            $host_0 = host(type: v4)
            # 172.16.8.8]
            $host_1 = host(type: v4)
        }

        steps {
            HTTP = tcp(src: $host_0, dst: $host_1, dst_port: 80)

            # POST /cgi-bin/setpsend.dll HTTP/1.0
            HTTP_POST_Client_Send = HTTP_Client_send {
                "POST /cgi-bin/setpsend.dll HTTP/1.0\r\n"
                "User-Agent: AAAAAAAAA\r\n"
                "Pragma: no-cache\r\n"
                "Proxy-Connection: Keep-Alive\r\n"
                "Host: e[HTTP_dst_ip]\r\n"
                header(header_name: "Content-length") {
                    length_string(of: content_1)
                }
                "\r\n"
                content_1 = "A"
            }

            # POST /cgi-bin/setpsend.dll HTTP/1.0
            HTTP_POST_Server_Receive = HTTP_POST_Client_Send.server_receive {
                assertions {
                    # Expect a POST message
                    /POST..HTTP/./
                }
            }

            HTTP_2 = tcp(src: $host_0, dst: $host_1, dst_port: 80)

            # POST /cgi-bin/setpsend.dll HTTP/1.0 Continuation or non-HTTP tr
            HTTP_2.POST_Client_Send = HTTP_2.Client_send {
                "POST /cgi-bin/setpsend.dll HTTP/1.0\r\n"
                "Accept: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
                "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\r\n"

```



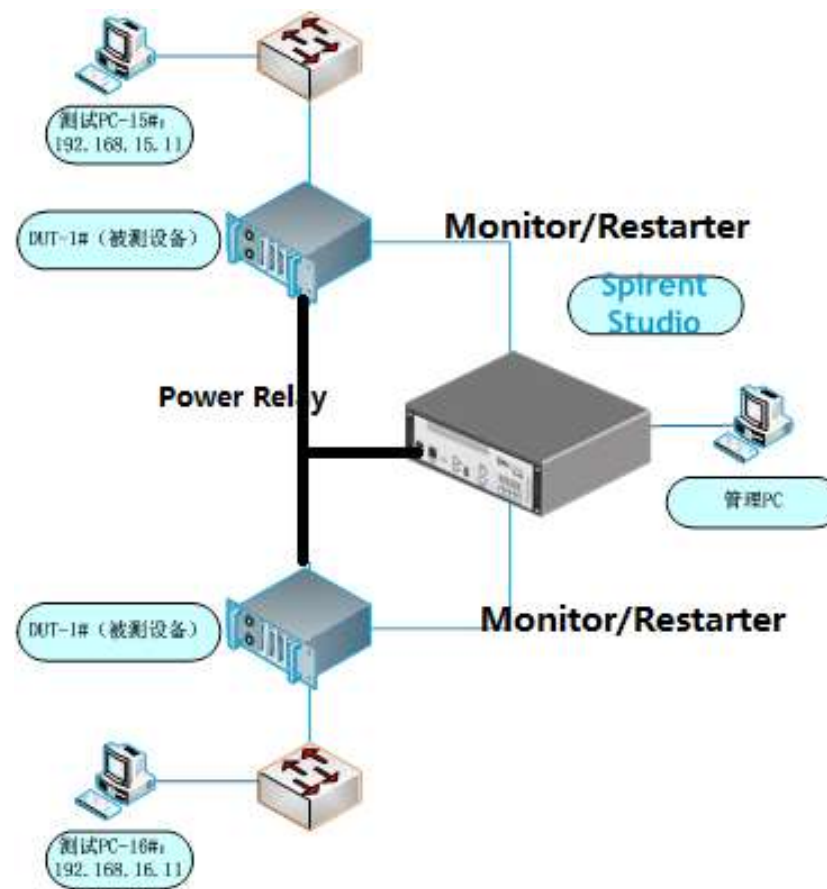
恶意软件（ Malware ）测试方法

- Malware是不断发展的测试类型，建议每周进行新的Malware测试
- 通过Spirent TestCloud数据库，同步最新的Malware攻击手法
- 通过一个测试端口，同时进行Malware和正常应用流量混合模拟
 - 混合各种应用流量和Malware，并确保Malware被阻断
 - 通过同时模拟大量的应用特征状态机和Malware，测试真实世界场景
- 对于隔离测试，模拟受感染主机行为
 - 基于有状态的MSL，Malware攻击不仅模拟核心攻击传送，而且可以模拟网络中受感染主机感染其它主机的行为
 - 当攻击开始被阻断时，则感染状态模拟也被阻止
- 高级根源分析
 - 分析系统显示未能被阻断的用户交互流程



未知漏洞挖掘工具 – Fuzzing/Mutation

- Fuzzing是进行未知漏洞挖掘/负面测试/健壮性测试的方法
- 在安全从业者保护用户的同时，黑客也在使用同样的方式寻找侵入的途径，这是一场无休止的竞赛，谁取得先机，谁就占据了主动
 - Protocol Mutation (基于原生协议)
 - Scenario Mutation (基于场景，私有协议)
 - 调试及控制工具：Restarter、Monitor、EVT (重置器，监视器，故障可重现程序)
 - 支持测试自动化

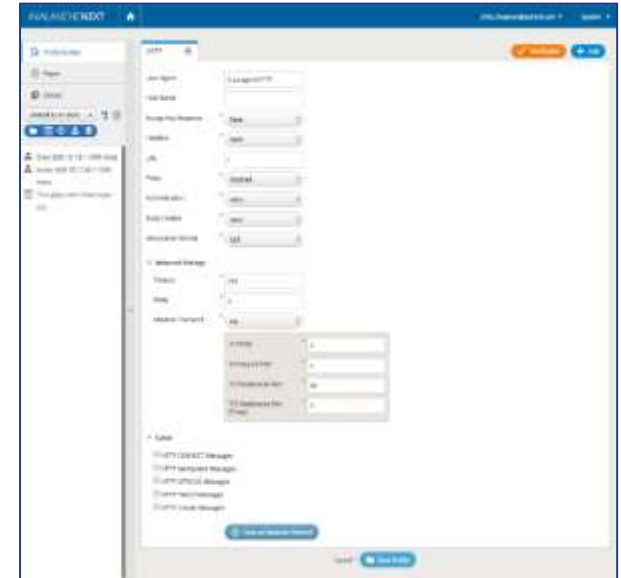


协议模糊攻击测试方法 – Protocol Mutation

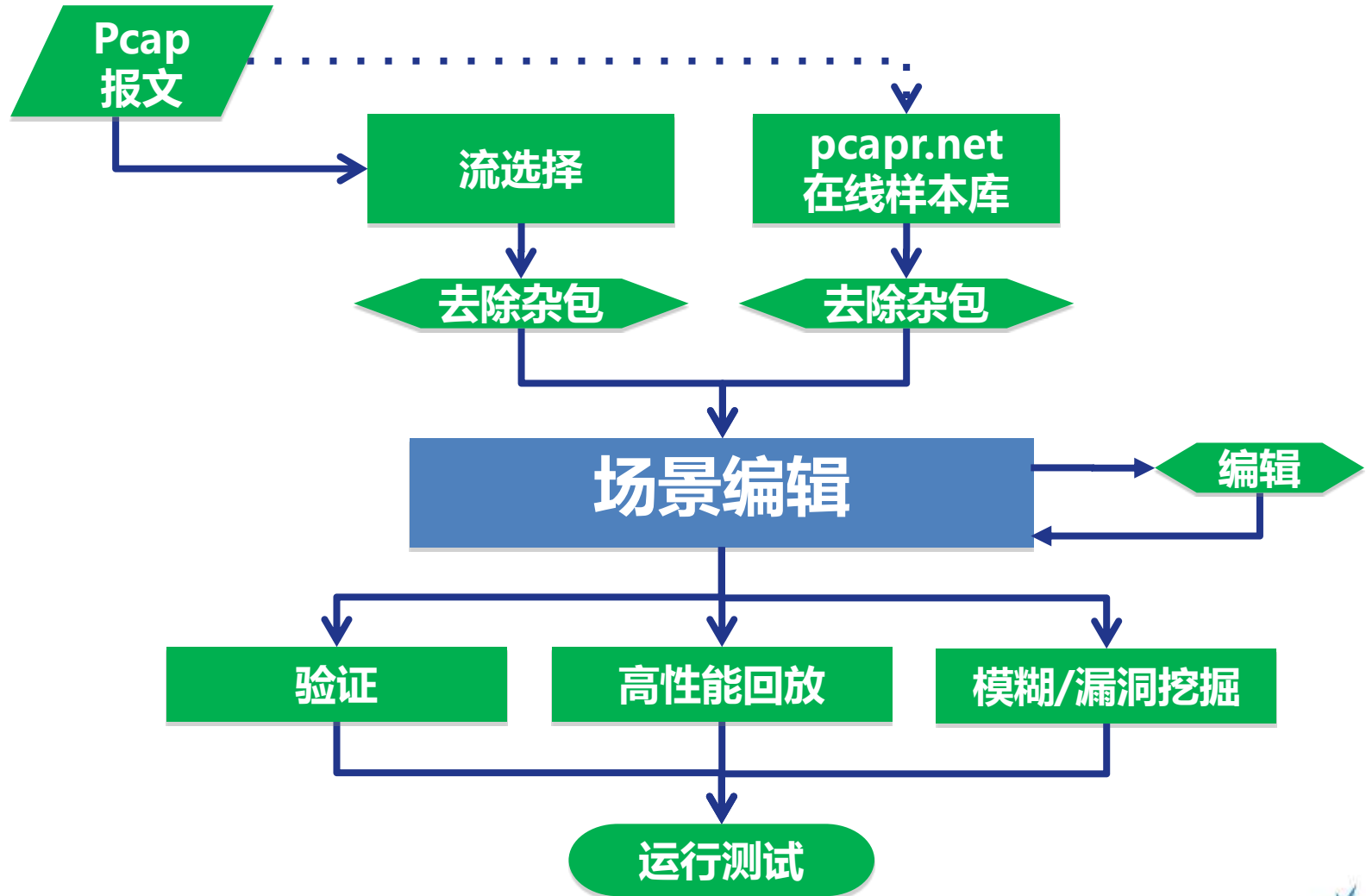
- 思博伦支持75种常见协议的Fuzzing测试，基于RFC协议标准，提供已经准备好的自动化协议测试机制。操作简单，不需要预备知识，只需要配置源和目标接口

- 主要协议举例

- 二层协议 – ARP、IEEE 802.1Q/X、PPPoE
- 三层协议 – IGMP、DHCPv4/6、IPv4/6、
- 路由协议 – BGP、OSPFv2/3、IS-IS、RIPv1/2、MPLS、VPLS
- VoIP 协议 – SIP、H.248、H.323
- 加密协议 – SSH、SSL、TLSv1/1.2、ISKAMP、IKEv2
- 工业控制协议 – IEC61850、MODBUS、DNP3 , MMS
- 应用层协议 – HTTP、SMTP、POP3、TELNET、LDAP
- AAA – RADIUS、DIAMETER、TACACS+
- 隧道协议 – VxLAN、GRE

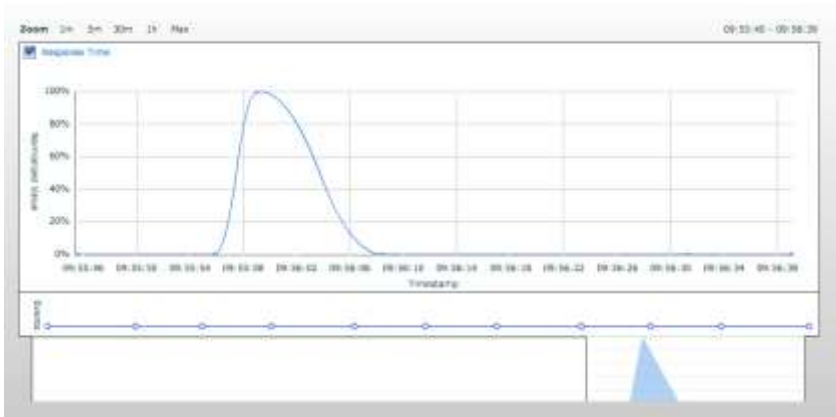
A screenshot of the 'SPIRENT VxLAN Mutation' tool interface. It displays a table with columns for 'VxLAN ID', 'VxLAN Name', 'VxLAN Type', 'VxLAN Size', 'VxLAN Time', 'VxLAN Mode', and 'VxLAN Action'. The table contains several rows of configuration data for VxLANs, including details like 'VxLAN ID', 'VxLAN Name', 'VxLAN Type', 'VxLAN Size', 'VxLAN Time', 'VxLAN Mode', and 'VxLAN Action'. The interface also includes a search bar and a 'Filter' button.

场景模糊攻击测试方法 – Scenario Mutation



模糊攻击测试结果分析报告

- 发生了什失败事件
- 哪里及什么时候出的问题
- 失败事件相关的状态机
- 保存故障重现条件，可迅速重现故障



Executive Summary Report: ManfredP_dns_assertions.pcap

Mo System User	admin	Product	Mo Test Suite (6.5.2.148322)
Start Date/Time	7/2/12 4:48:35 AM	Mo System IP	172.16.1.54
Duration	6 minutes 31 seconds 301 milliseconds	Mo System Serial #	0203-0711-0000-208E

Detection Effectiveness of Target

Detection Effectiveness Against Traffic Variations



Test	Missed	Blocked	Effectiveness
ManfredP_dns_assertions.pcap	6,838	478	6.534%

Traffic Variation Results (Scenarios)



The target was analyzed using **7,317 variations** (generated from 174 test cases in 1 scenario). The target was **available for 5 minutes 48 seconds 784 milliseconds** during the attacks and was **unavailable for 0 milliseconds**.

Total Tests Run	174 test cases were run
Passed	174 test cases passed
Failed	0 test cases failed

Test	Statistics										
ManfredP_dns_assertions.pcap	<table><tr><td>Protocol Scenario</td><td>ManfredP_dns_assertions.pcap</td></tr><tr><td>Availability</td><td>100.000%</td></tr><tr><td>Faults</td><td>No faults were found</td></tr><tr><td>Variations</td><td>7317</td></tr><tr><td>Coverage</td><td></td></tr></table>	Protocol Scenario	ManfredP_dns_assertions.pcap	Availability	100.000%	Faults	No faults were found	Variations	7317	Coverage	
Protocol Scenario	ManfredP_dns_assertions.pcap										
Availability	100.000%										
Faults	No faults were found										
Variations	7317										
Coverage											

网络攻击测试方法小结

- 攻击可以源自不同IP地址/MAC地址、甚至不同子网（通过VR）
- 在接入协议（PPPoE、DHCP）后发送攻击流量
- 在IPSec隧道上发送攻击流量
- 同时从多个测试端口发送大量攻击流量，并且真正做到分布式模拟
- 从同一个测试端口，同时发送攻击流量和正常应用流量混合
- 在攻击测试中加入网络损伤元素（丢包、延迟，等）
- 大量IPv6攻击仿真
- 零天（Zero-day）攻击 — 攻击库（Knowledge Base）更新迅速
- Attack Designer – 可以构造任意攻击手法
- Malware测试
- 未知攻击模拟 – Protocol Mutation、Scenario Mutation

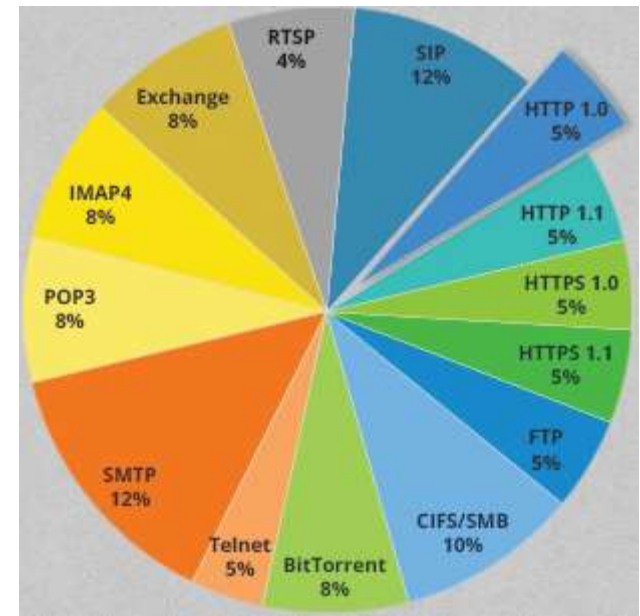


为什么测试中需要攻击流量和正常流量混合？

- 一些安全设备在单纯的攻击流量环境中，可以阻断所有攻击，但是当环境中同时混合了攻击流量和正常流量的时候，这些设备就会漏报一些攻击
- 在真实的网络中，没有单纯的攻击流量，所有的攻击都是和其它流量混合在一起的
- [RFC 3511] 5.5 Denial Of Service Handling – To determine the **effect** of a denial of service attack **on a DUT/SUT TCP connection establishment and/or HTTP transfer rates.**
- 网络安全设备测试的三个步骤：
 - 参考RFC 3511，测试安全设备的基准性能指标（并发TCP连接数、最大TCP连接建立速率，等）
 - 攻击流量性能测试
 - 攻击流量与正常流量混合 — 检查安全设备在检测和阻断攻击流量的同时，不影响其对正常流量的转发（无性能损耗）

为什么要进行真实网络环境下的攻击仿真测试？

- [RFC 3511] 扩展：
 - 不只看攻击流量对单一应用协议的影响
 - 不只看攻击流量对TCP连接建立和HTTP Goodput的影响
 - 需要看攻击流量在特定应用流量模型下的表现
- 相比之前的“攻击流量和正常流量混合”的测试方法，对正常流量部分的模拟有了更高的要求
- 需要根据不同的应用场景，建立不同的流量模型，然后测试攻击流量在不同流量模型下，对安全设备或者网络处理应用性能的影响



思博伦下一代网络安全测试方案

Avalanche NEXT

- 基于Web浏览器的多用户界面
- 最新应用和攻击内容测试
(Spirent TestCloud : 4000多种场景)
- 高性能：千万级并发连接数；百万级TCP连接建立速率 (CPS)
- 攻击/已知漏洞测试
- 模糊攻击 (Fuzzing) 测试
- Malware仿真测试
- 测试方法学 (RFC 3511)
 - HTTP CPS
 - HTTP 并发连接数
 - HTTP & E-Mix吞吐量测试



Avalanche NEXT

- 面向测试方法学的多用户界面

The screenshot displays the Avalanche NEXT web application interface. At the top is a dark blue header bar containing the 'AVALANCHENEXT' logo, a home icon, the user email 'haisheng.wang@spirent.com', and navigation links for 'System' and 'Help'. A status indicator shows 'INTERNET' is connected. The main content area has a light gray background with the text 'Welcome. Choose a Test Template to Get Started.' Below this, there are two columns of test templates. The left column is titled 'Audit / Performance Tests' and includes sub-links for 'Store', 'Player', and 'Library'. It contains three templates: 'CyberSecurity Assessment' (with a checkmark icon), 'Application Identification' (with a line graph icon), and 'Reliability Testing' (with a clock icon). The right column is titled 'Protocol Tests' and includes sub-links for 'Profile Builder', 'Player', and 'Library'. It contains six templates: 'Throughput with Mixed Apps' (with a pie chart icon), 'HTTP 1.1 Throughput' (with a speedometer icon), 'Max HTTP 1.1 Throughput' (with a speedometer icon), 'HTTP 1.0 Connection Per Second' (with a wrench icon), 'Max HTTP Open Connections' (with a globe icon), and 'Fuzzing' (with a robot icon).

AVALANCHENEXT | | haisheng.wang@spirent.com | System | Help | INTERNET

Welcome. Choose a Test Template to Get Started.

Audit / Performance Tests

Store | Player | Library

- CyberSecurity Assessment**
Run over ten thousand modern and advanced instances of attacks and malware
- Application Identification**
Create high volumes of the latest mobile and cloud applications, as well as security traffic patterns
- Reliability Testing**
Perform long-duration tests with the full Spirent TestCloud application load

Protocol Tests

Profile Builder | Player | Library

- Throughput with Mixed Apps**
Create and run tests with preconfigured Enterprise traffic Mix to achieve high throughput
- HTTP 1.1 Throughput**
Create scalable HTTP tests with different object sizes to achieve line-rate throughput
- Max HTTP 1.1 Throughput**
Create maximum bandwidth tests with the ability to test both uni-directional and bi-directional.
- HTTP 1.0 Connection Per Second**
Create tests to achieve industry's highest state generator with Extreme Scale and Performance module (ESP)
- Max HTTP Open Connections**
Create tests to achieve huge levels of HTTP open connections. Testing the maximum scalability & performance of the DUT.
- Fuzzing**
Perform different service and protocol mutation scenarios through FUZZ player

测试对象

- ◉ 防火墙、应用防火墙、下一代防火墙
- ◉ 深度包检测设备（DPI）、统一威胁管理平台（UTM）
- ◉ 入侵检测系统/入侵防护系统（IDS/IPS）
- ◉ VPN网关（IPSec VPN、SSL VPN）
- ◉ 4-7层交换机、服务器负载均衡器（SLB）
- ◉ 网络缓存、代理缓存、Reverse-Proxy
- ◉ URL过滤设备、内容过滤器、SMTP中继
- ◉ 防病毒系统、反垃圾邮件系统、防间谍软件系统、防Malware系统
- ◉ SSL加速器、HTTP/HTTPS加速器
- ◉ 网络存储测试
- ◉ 数据库安全测试
- ◉ 各种应用网关及IPv6支持

下一代网络安全测试方法总结

- 攻击仿真测试：已知攻击、未知攻击（Fuzzing）、恶意软件模拟
- 已知攻击测试手法更新：
 - 客户化定制攻击手法 – Attack Designer
 - 定期升级 – TestCloud、Knowledge Base
- 未知攻击测试 – 模糊攻击测试
 - 已知协议Fuzzing测试 – Protocol Mutation
 - 私有协议Fuzzing测试 – Scenario Mutation
- 海量应用仿真测试：SAPEE、TestCloud
- 高性能测试：千万级并发连接数、百万级新建连接速率、线速应用流量仿真
- 应用流量和攻击流量混合，模拟真实网络场景，赛博靶场（Cyber Range）
- 安全协议（IPSec、SSL）性能测试
- 云安全测试 – Virtual方案





谢 谢

