CyberFlood 简明操作手册

任红波

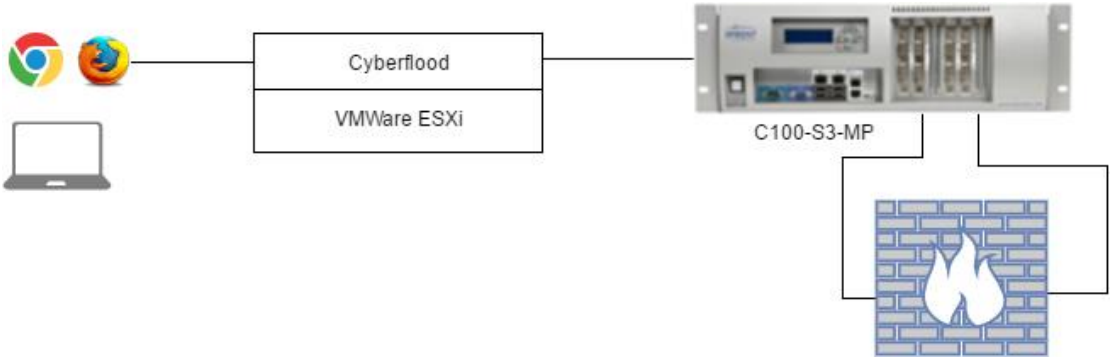
Hongbo.ren@spirent.com

2018.3

1. 准备篇

CyberFlood 组网

CyberFlood 是部署并运行在虚拟机中的软件，控制 C100-S3-MP 等硬件。使用最新版的谷歌、火狐或者 Safari 浏览器访问，不支持 IE 浏览器。



登录系统

使用 https://CyberFlood 控制器 IP 登录系统。因为使用了自签名证书，如果提示不受支持，点击继续前往。

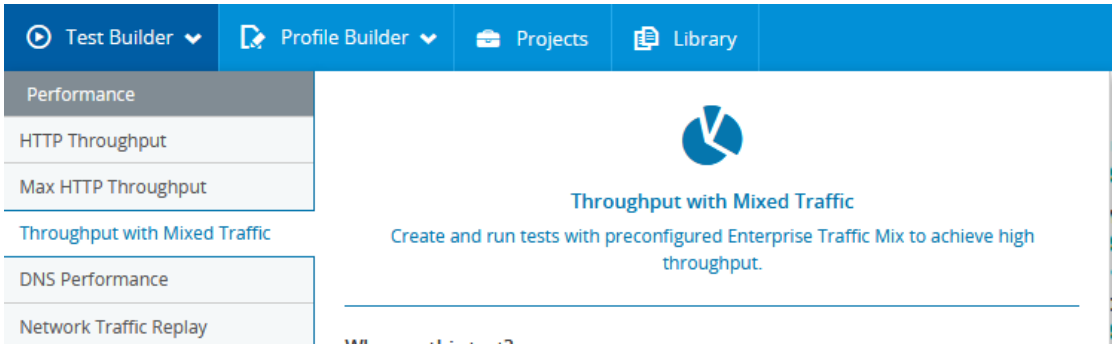
登录用户名和密码

请询问系统管理员。

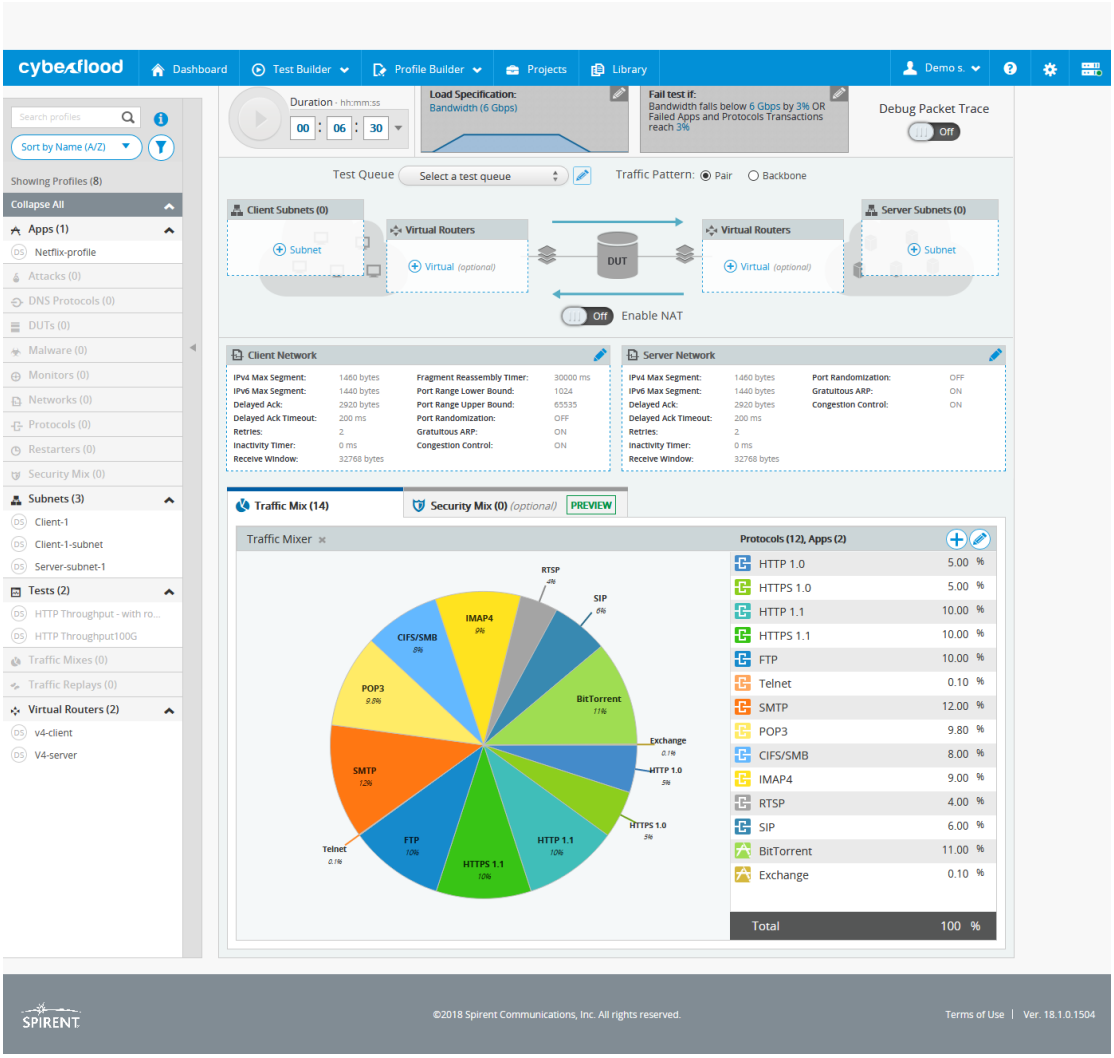
2. 配置混合流量测试（eMix）

配置混合流量测试

在 Test Builder 里面选择 Throughput With Mixed Traffic 模板，点击 Build a New Test 开始一个新的测试。



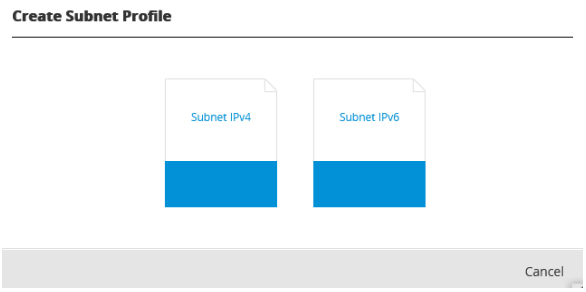
默认的配置如下。



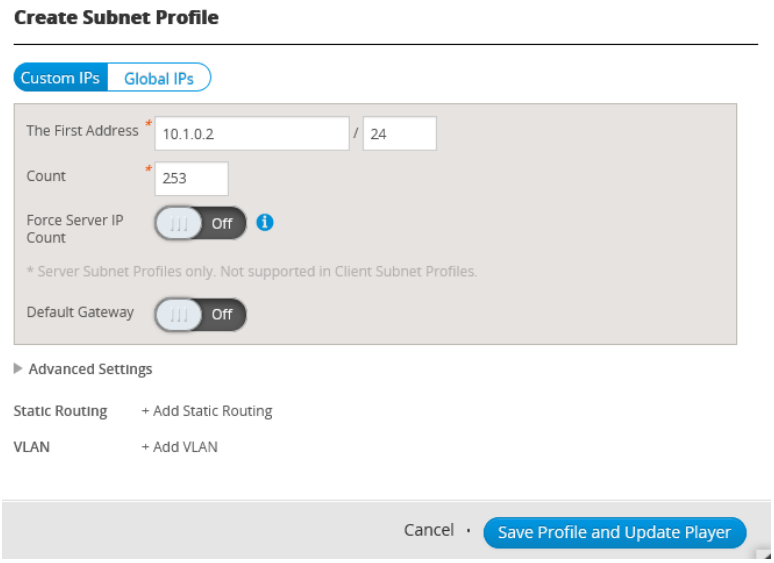
在 Test Queue 里面通过下拉框选择 Brave 队列。

在 Client Subnets 配置子网。有 2 种方法，一种是点击 Subnet 配置一个新的子网，另一种是从左边拖拽一个 subnet 到 Client Subnets 中。

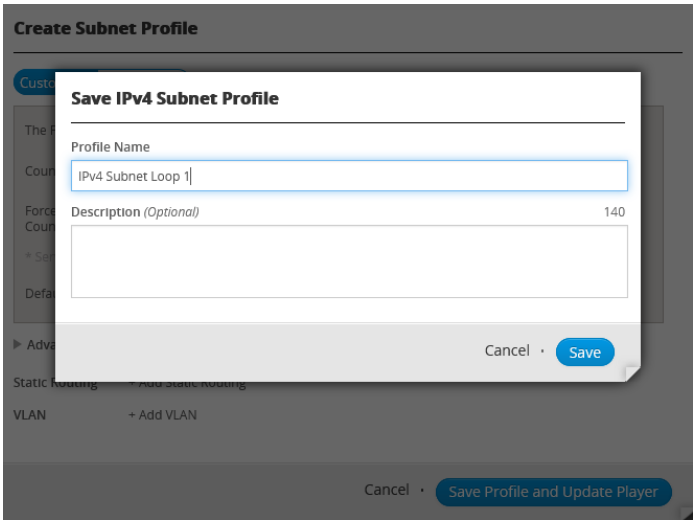
如果是点击 Subnet 配置了子网，进入如下画面配置：



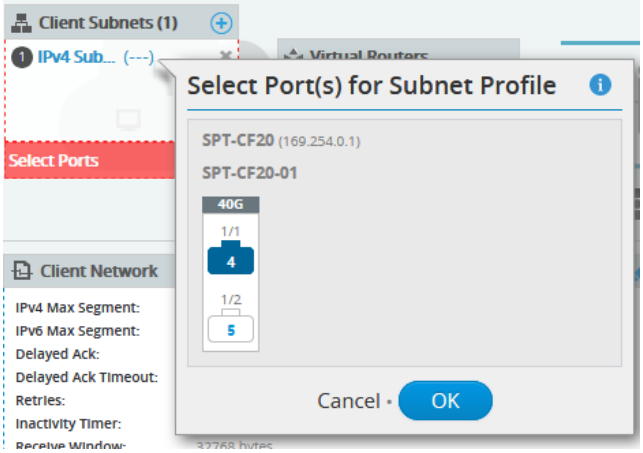
选择 Subnet IPv4，并配置网络信息和 vlan 等。



保存配置

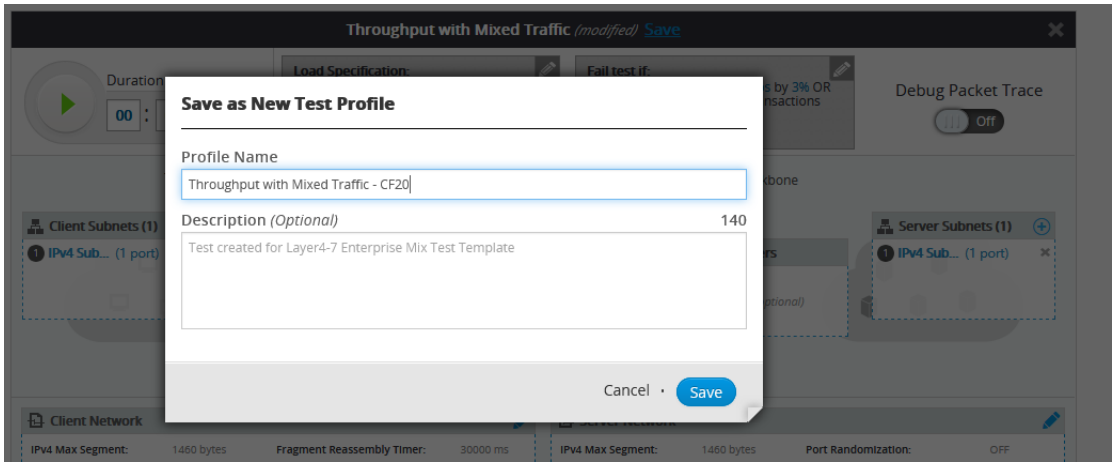


分配测试仪端口，如果没有出现端口画面，点击（---）。把 1/1 端口分配给客户端。



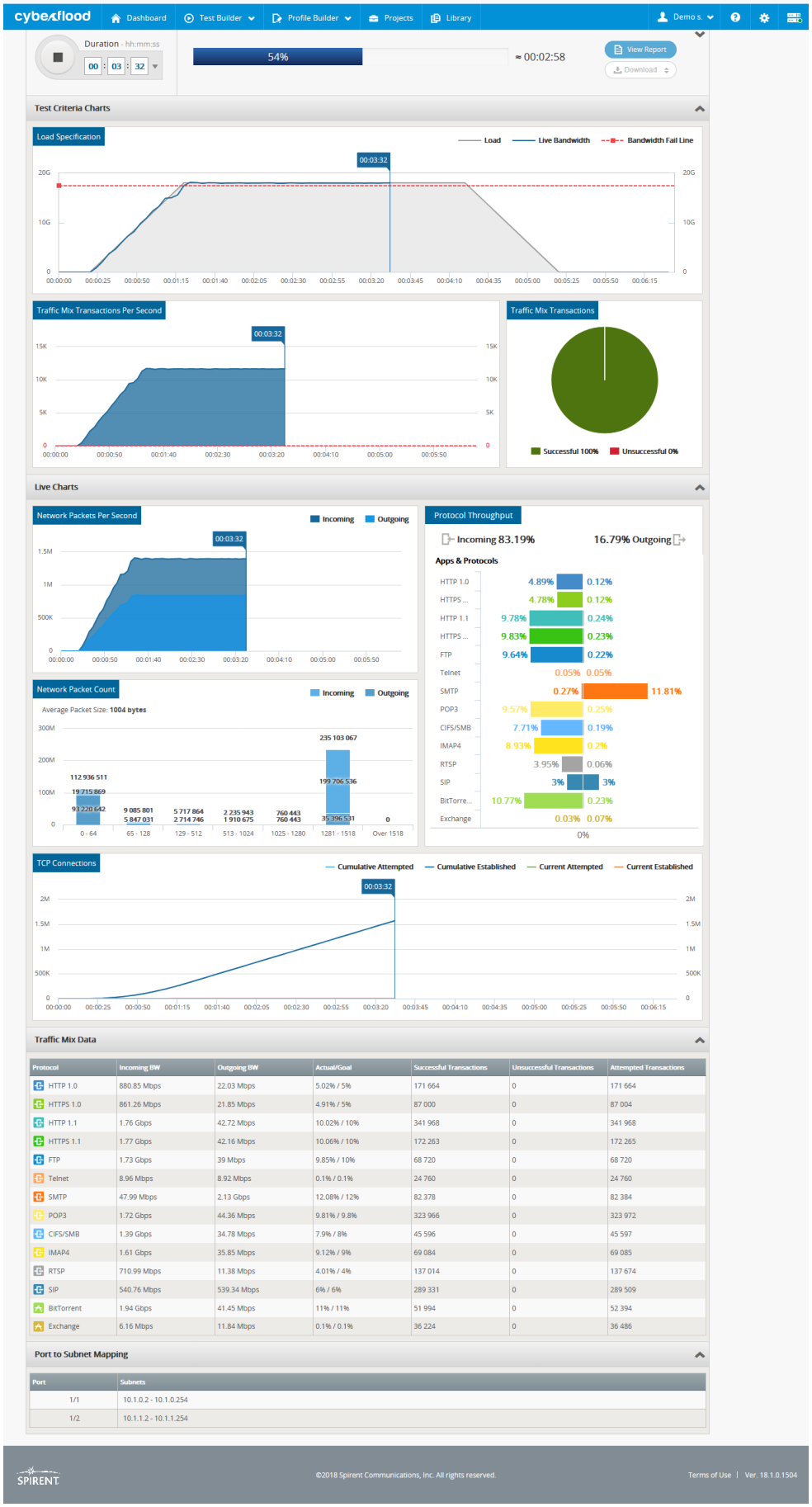
同样的，建立服务器侧子网 IPv4 Subnet Loop 2，并分配端口。注意两个子网地址不要重复。

保存配置



运行并查看结果

点击绿色的三角开始运行。运行状态如下：



Protocol	Incoming BW	Outgoing BW	Actual/Goal	Successful Transactions	Unsuccessful Transactions	Attempted Transactions
HTTP 1.0	880.85 Mbps	22.03 Mbps	5.02% / 5%	171 664	0	171 664
HTTPS 1.0	861.26 Mbps	21.85 Mbps	4.91% / 5%	87 000	0	87 004
HTTP 1.1	1.76 Gbps	42.72 Mbps	10.02% / 10%	341 968	0	341 968
HTTPS 1.1	1.77 Gbps	42.16 Mbps	10.06% / 10%	172 263	0	172 265
FTP	1.73 Gbps	39 Mbps	9.85% / 10%	68 720	0	68 720
Telnet	8.96 Mbps	8.92 Mbps	0.1% / 0.1%	24 760	0	24 760
SMTP	47.99 Mbps	2.13 Gbps	12.08% / 12%	82 378	0	82 384
POP3	1.72 Gbps	44.36 Mbps	9.81% / 9.8%	323 966	0	323 972
CIFS/SMB	1.39 Gbps	34.78 Mbps	7.9% / 8%	45 596	0	45 597
IMAP4	1.61 Gbps	35.85 Mbps	9.12% / 9%	69 084	0	69 085
RTSP	710.99 Mbps	11.38 Mbps	4.01% / 4%	137 014	0	137 674
SIP	540.76 Mbps	539.34 Mbps	6% / 6%	289 331	0	289 509
BitTorrent	1.94 Gbps	41.45 Mbps	11% / 11%	51 994	0	52 394
Exchange	6.16 Mbps	11.84 Mbps	0.1% / 0.1%	36 224	0	36 486

Port	Subnets
1/1	10.1.0.2 - 10.1.0.254
1/2	10.1.1.2 - 10.1.1.254

测试报告

测试结束后点击 View Report 生成测试报告。

cybexflood

Throughput with Mixed Traffic - CF20

PDF Print

TESTED BY SPIRENT

A*

Actual bandwidth **never fell below** the specified goal of **3% of 18 Gbps** over the total duration** of the test. Apps and Protocols Transactions **never fell below** the specified goal of **3% of Total Apps and Protocols Transactions** over the total duration** of the test.

* This score is calculated by taking the Pass/Fail criteria goals defined in the test and measuring if they fell below the minimum requirement set and averaging. The amount of time data fell below that goal. A = 90% and above, B = 80% - 89%, C = 70% - 79%, D = 60% - 69%, F = 59% and below.
** Duration is the total test time, excluding everything up to the Ramp-up and after the Ramp-down.

Summary

Created By	Test Name	Number Of Traffic Mix
demo@spirent.com	Throughput with Mixed Traffic - CF20	14
	Description	

Queue Name	Started at	Finished at	Vol. for Server Bandwidth	Measurement
Brave	2018-3-19 11:09:25	2018-3-19 11:17:15	18 Gbps	Bandwidth

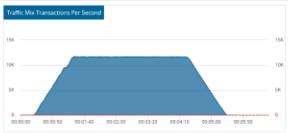
Client Sent	Server Received	Server Sent	Client Received	Average Throughput
90.72 GB	90.72 GB	453.42 GB	453.42 GB	17.95 Gbps

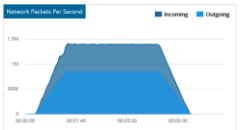
Traffic Mix		
Executed	Passed	Failed
2 822 090 Connections	100% (2 822 090 Connections)	0% (0 Connections)

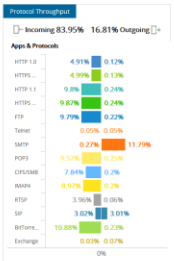
Network Profile Configuration

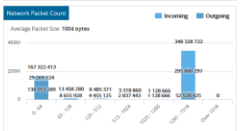
Client Network		Server Network	
IPv4 Max Segment:	1460 B	IPv4 Max Segment:	1460 B
IPv6 Max Segment:	1440 B	IPv6 Max Segment:	1440 B
Receive Window:	32768 B	Receive Window:	32768 B
Retries:	2	Retries:	2
Delayed Ack Timeout:	200 ms	Delayed Ack Timeout:	200 ms
Delayed Ack:	2920 B	Delayed Ack:	2920 B
Port Range:	1024 - 65535		

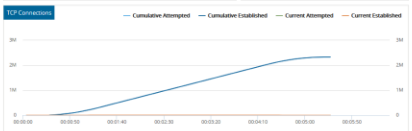
Charts











Traffic Mix Data

Protocol	Incoming BW	Outgoing BW	Actual/Goal	Successful Transactions	Unsuccessful Transactions	Attempted Transactions
HTTP 1.0	884.63 Mbps	22.12 Mbps	5.04%/5%	254 560	0	254 560
HTTPS 1.0	898.55 Mbps	22.79 Mbps	5.12%/5%	128 512	0	128 512
HTTP 1.1	1.76 Gbps	42.8 Mbps	10.03%/10%	507 872	0	507 872
HTTPS 1.1	1.78 Gbps	42.38 Mbps	10.11%/10%	255 040	0	255 040
FTP	1.76 Gbps	39.64 Mbps	10.01%/10%	101 488	0	101 488
Telnet	9.03 Mbps	9.07 Mbps	0.1%/0.1%	36 648	0	36 648
SMTP	47.88 Mbps	2.12 Gbps	12.05%/12%	122 264	0	122 264
POP3	1.72 Gbps	44.39 Mbps	9.82%/9.8%	480 800	0	480 800
CIFS/SMB	1.41 Gbps	35.38 Mbps	8.03%/8%	67 608	0	67 608
IMAP4	1.61 Gbps	36.07 Mbps	9.17%/9%	102 032	0	102 032
RTSP	712.37 Mbps	11.4 Mbps	4.02%/4%	204 816	0	204 816
SIP	543.91 Mbps	542.53 Mbps	6.04%/6%	429 206	0	429 206
BitTorrent	1.96 Gbps	41.91 Mbps	11.12%/11%	77 204	0	77 204
Exchange	6.18 Mbps	11.87 Mbps	0.1%/0.1%	54 040	0	54 040

Port Interfaces

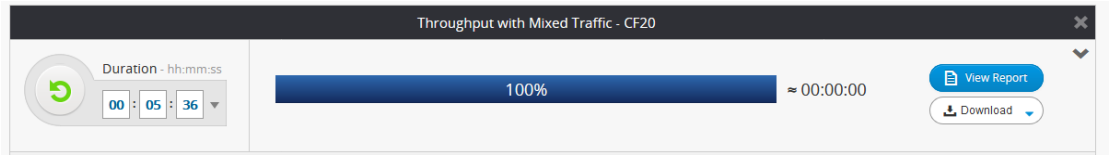
Port Interface	Protocol	Incoming BW	Outgoing BW	Actual/Goal	Successful Transactions	Unsuccessful Transactions	Attempted Transactions
1/1	HTTP 1.0	884.63 Mbps	22.12 Mbps	5.04%/5%	254 560	0	254 560
	HTTPS 1.0	898.55 Mbps	22.79 Mbps	5.12%/5%	128 512	0	128 512
	HTTP 1.1	1.76 Gbps	42.8 Mbps	10.03%/10%	507 872	0	507 872
	HTTPS 1.1	1.78 Gbps	42.38 Mbps	10.11%/10%	255 040	0	255 040
	FTP	1.76 Gbps	39.64 Mbps	10.01%/10%	101 488	0	101 488
	Telnet	9.03 Mbps	9.07 Mbps	0.1%/0.1%	36 648	0	36 648
	SMTP	47.88 Mbps	2.12 Gbps	12.05%/12%	122 264	0	122 264
	POP3	1.72 Gbps	44.39 Mbps	9.82%/9.8%	480 800	0	480 800
	CIFS/SMB	1.41 Gbps	35.38 Mbps	8.03%/8%	67 608	0	67 608
	IMAP4	1.61 Gbps	36.07 Mbps	9.17%/9%	102 032	0	102 032
	RTSP	712.37 Mbps	11.4 Mbps	4.02%/4%	204 816	0	204 816
	SIP	543.91 Mbps	542.53 Mbps	6.04%/6%	429 206	0	429 206
	BitTorrent	1.96 Gbps	41.91 Mbps	11.12%/11%	77 204	0	77 204
	Exchange	6.18 Mbps	11.87 Mbps	0.1%/0.1%	54 040	0	54 040

Port to Subnet Mapping

Port	Subnets
1/1	10.1.0.2 - 10.1.0.254
1/2	10.1.1.2 - 10.1.1.254

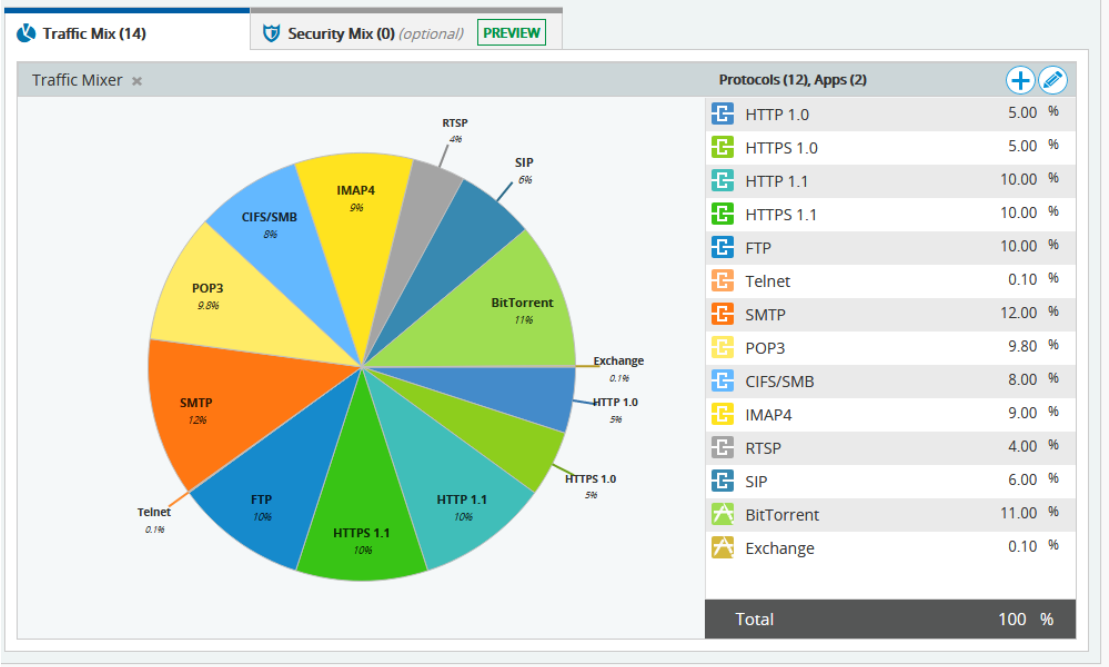
测试重新运行和编辑

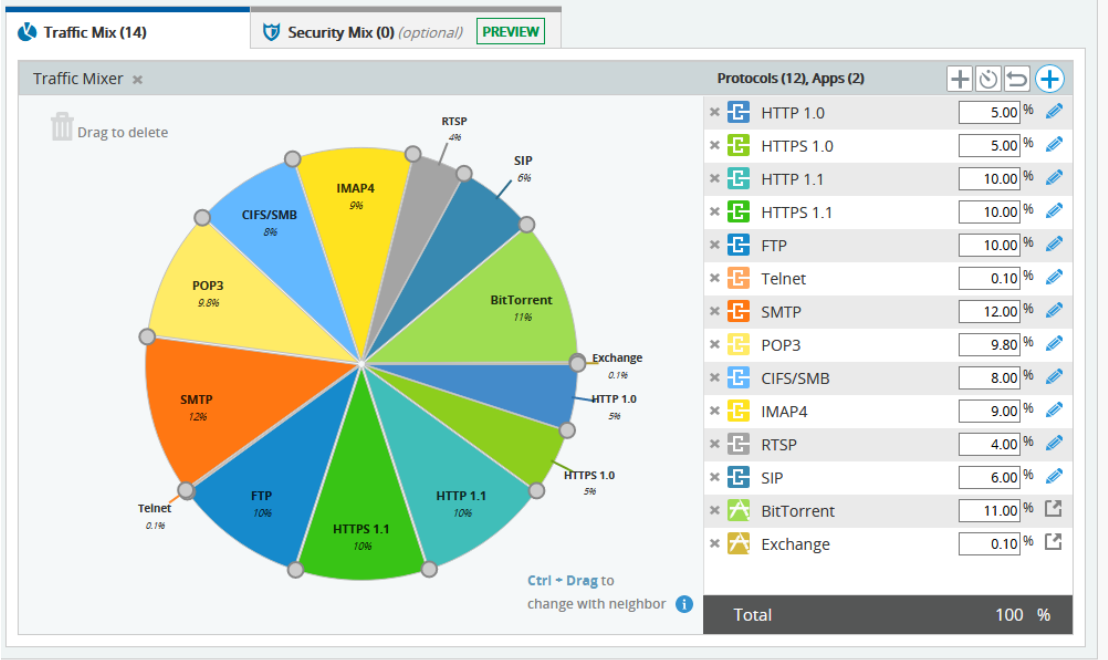
测试结束后，点击绿色的循环按钮可以重跑一遍测试。点击右上角的 X 返回并编辑测试配置。



增加应用场景

点击右上角的铅笔图标编辑业务配置。





增加新应用。

里面的 X 删除应用，铅笔编辑或者查看配置。

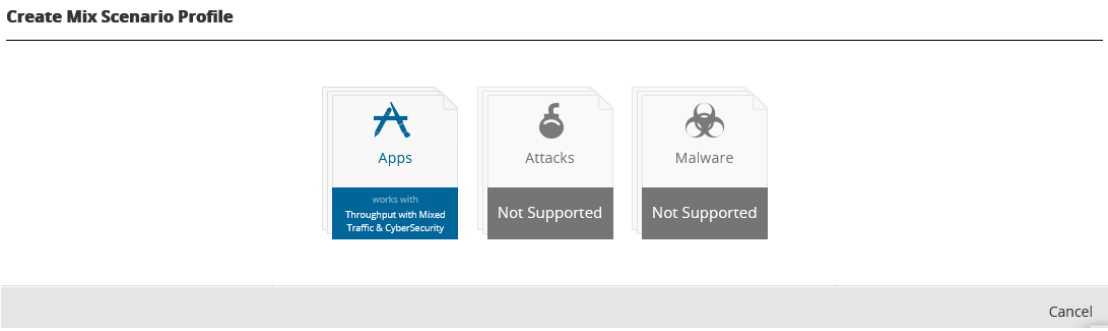
退出

撤销

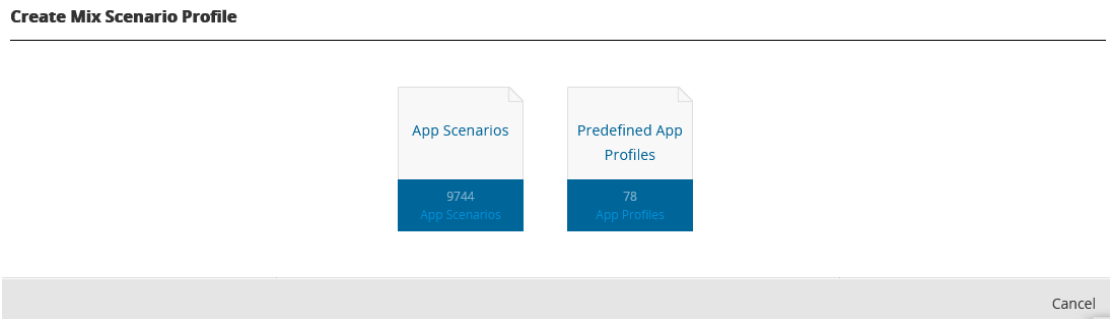
增加应用

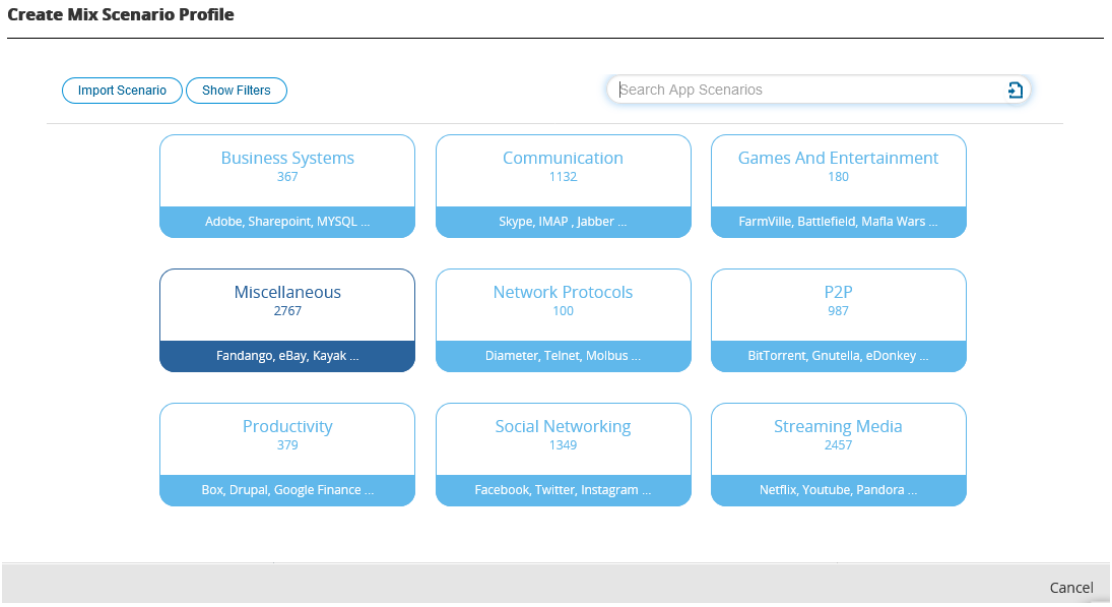
以增加微信业务为例：

点击进入应用选择，点击 APPS。

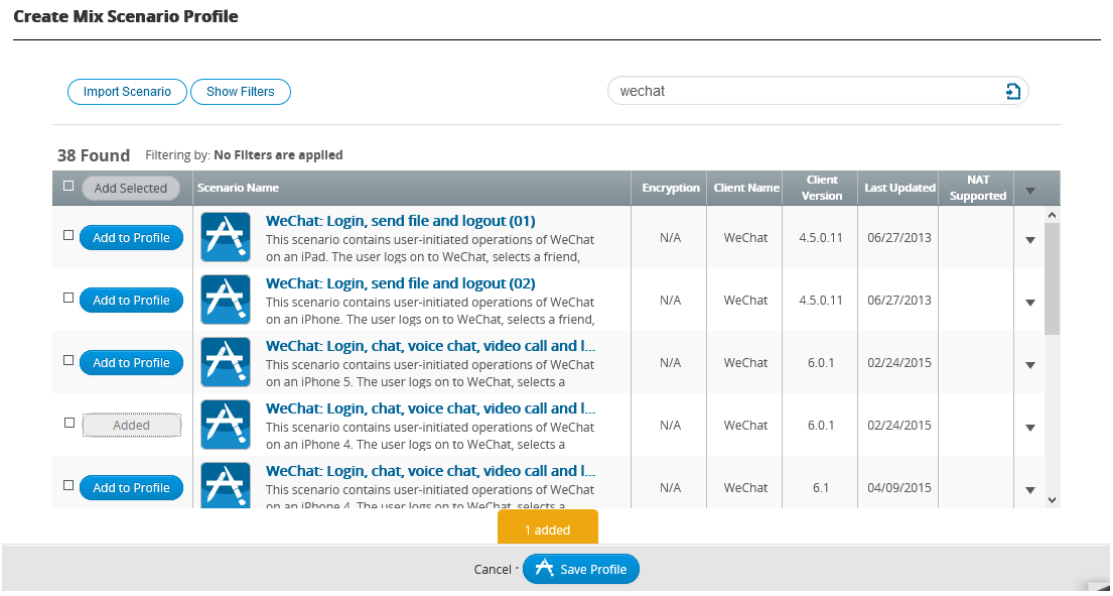


进入 App Scenarios

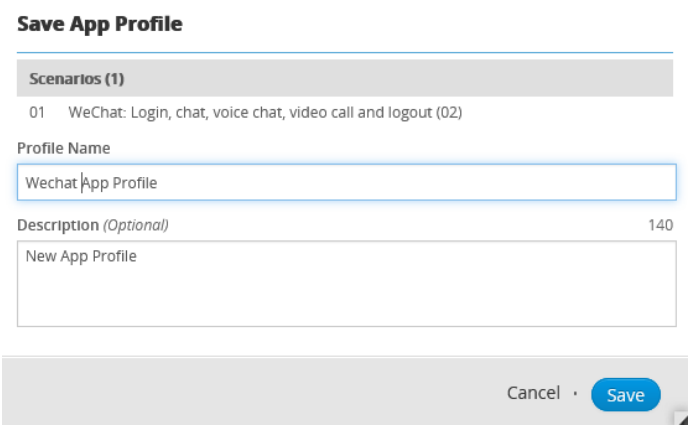




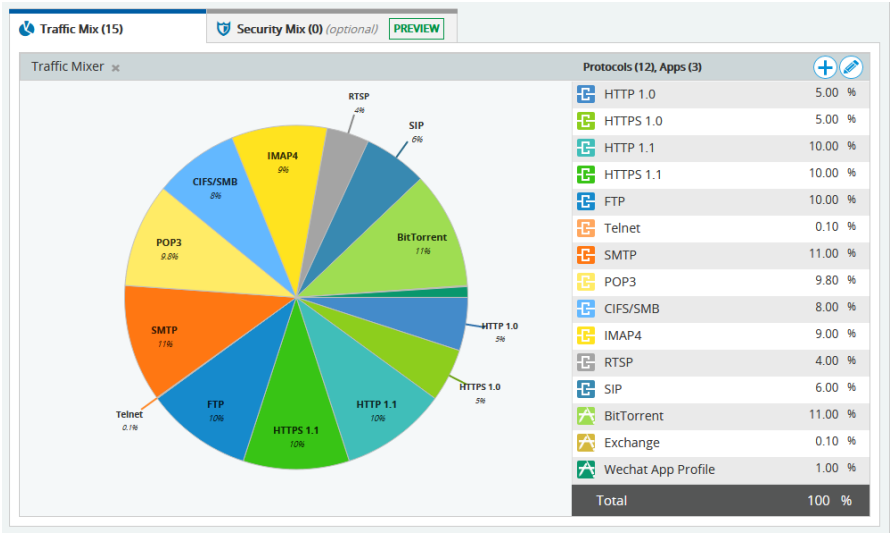
搜索 wechat,



选中需要的场景并点击 Add to Profile，保存为 Wechat App Profile。



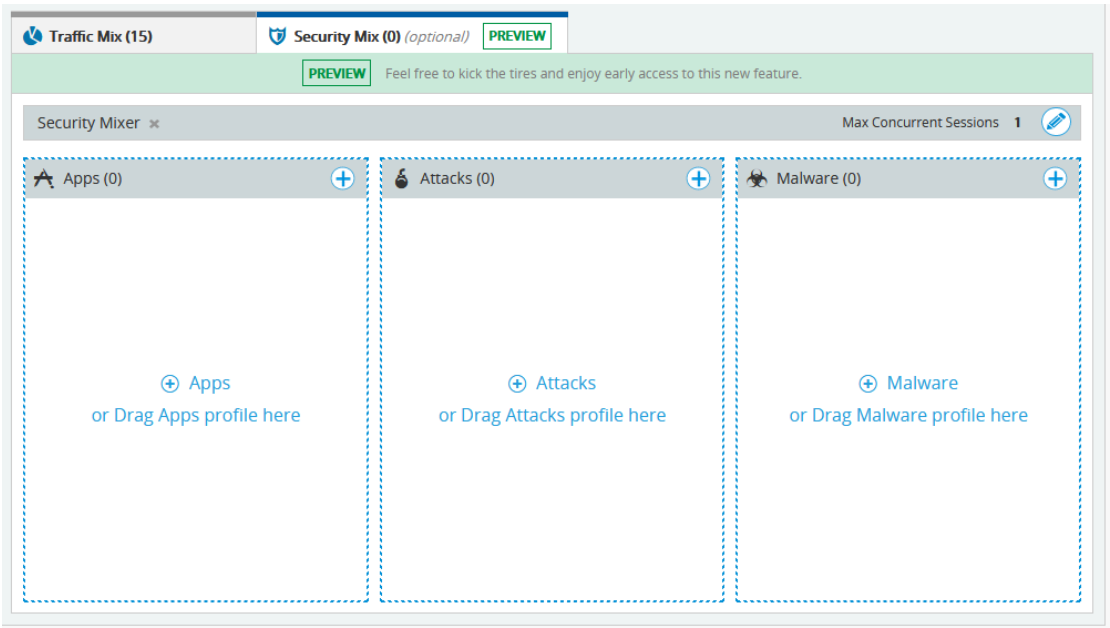
可以看到应用中多了微信场景。



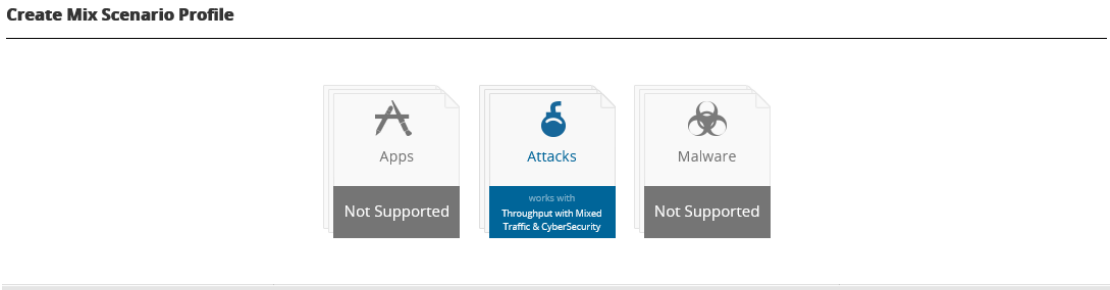
增加网络攻击和恶意软件

除了混合多种应用之外，也可以混合攻击病毒等内容。

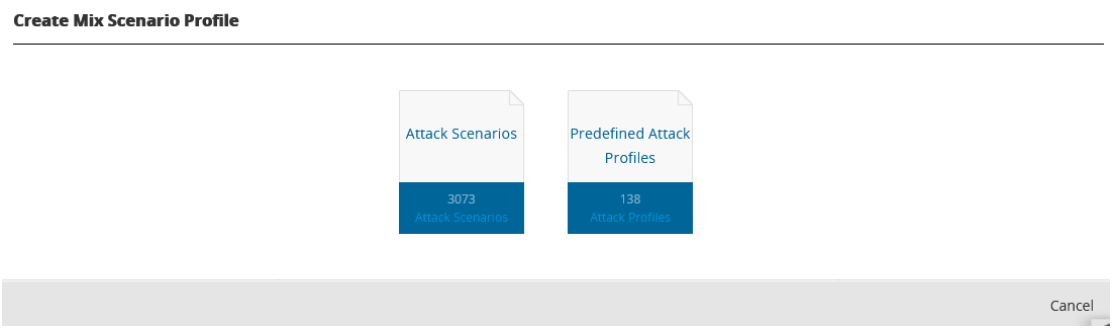
进入 Security Mix

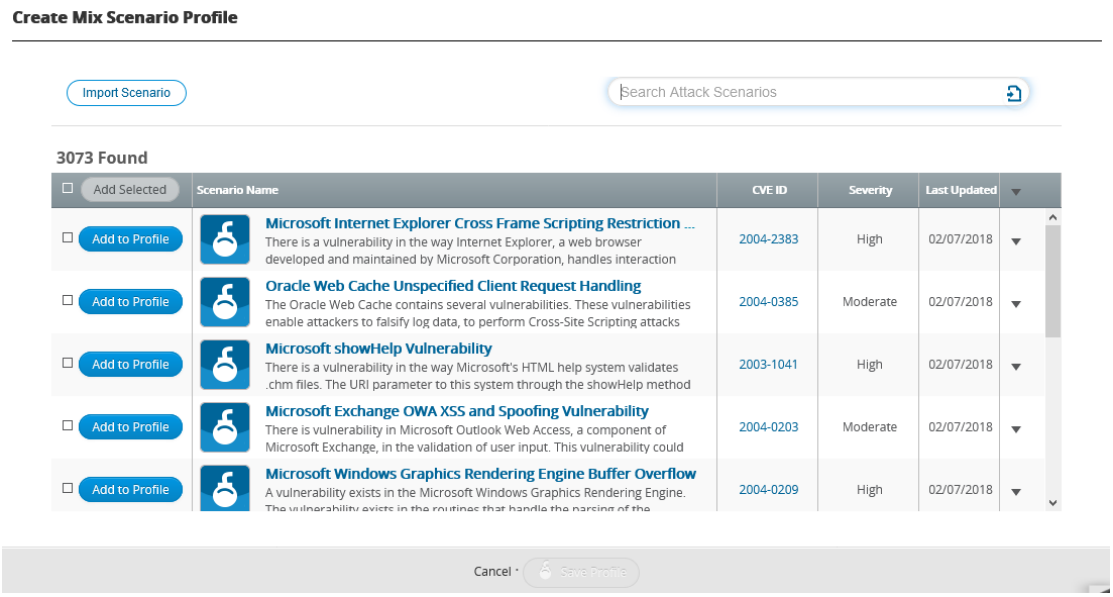


点击+ Attacks 增加攻击内容。

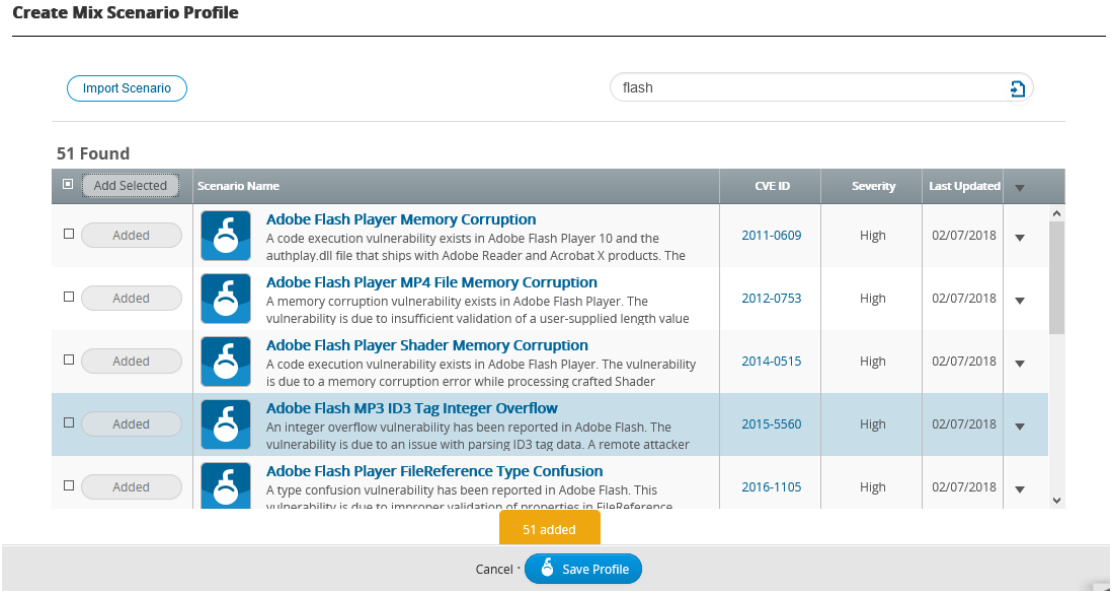


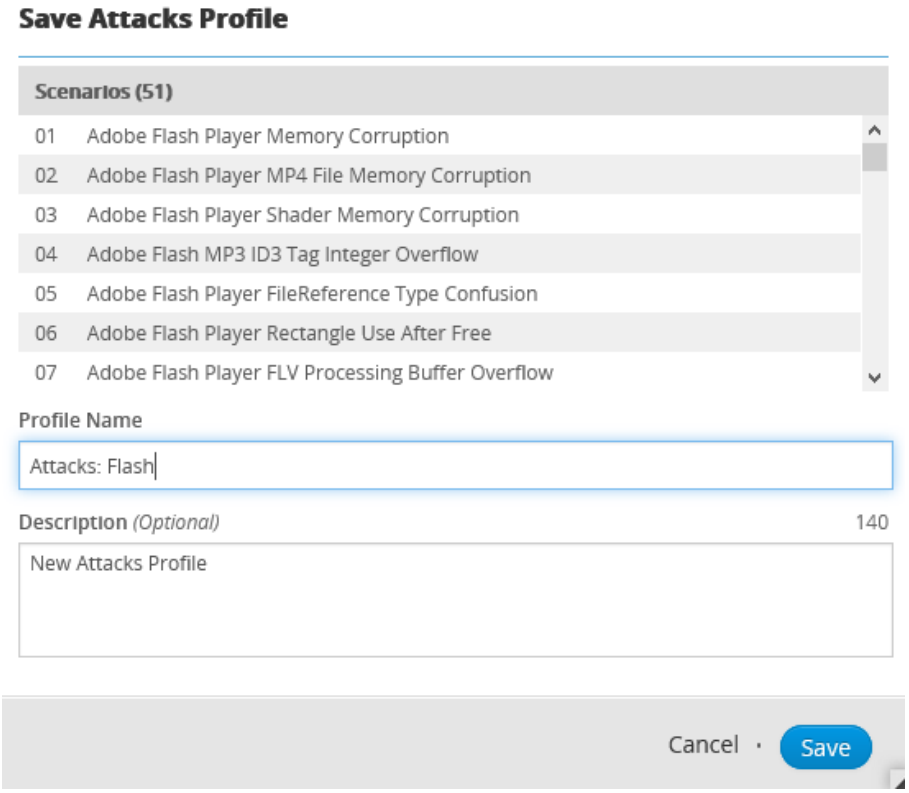
选择 Attack Scenarios



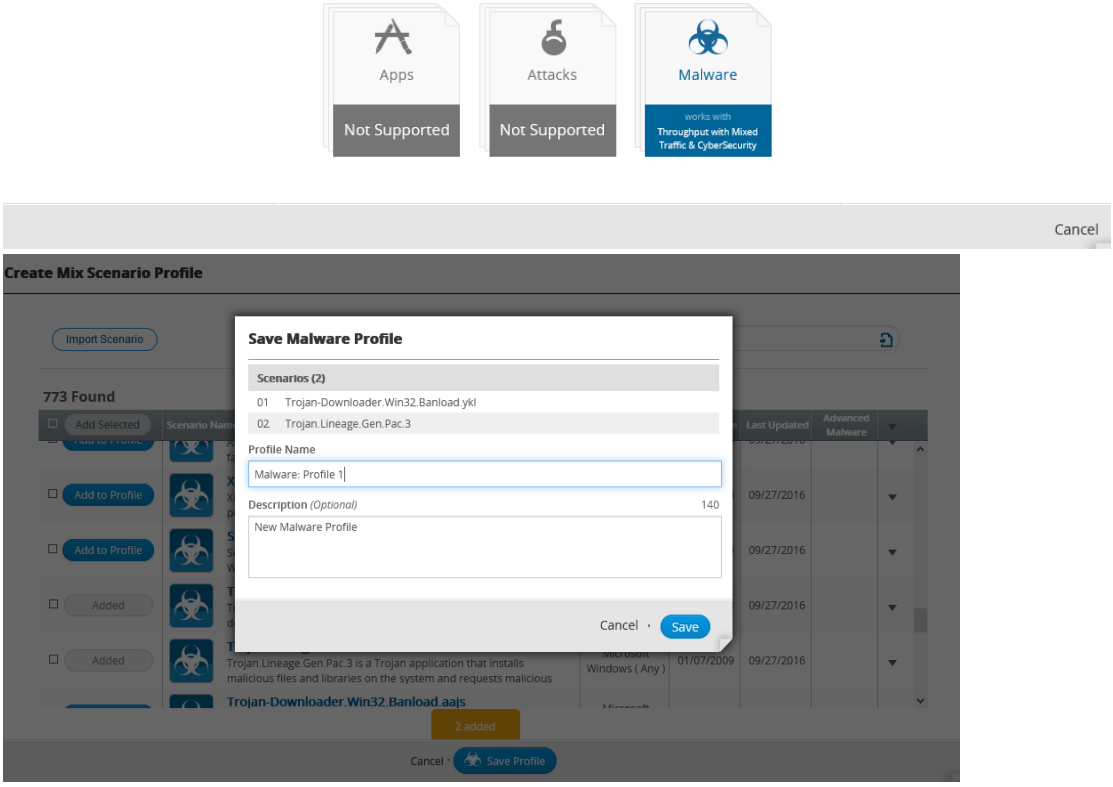


搜索 Flash，找到 51 种，选择并保存。

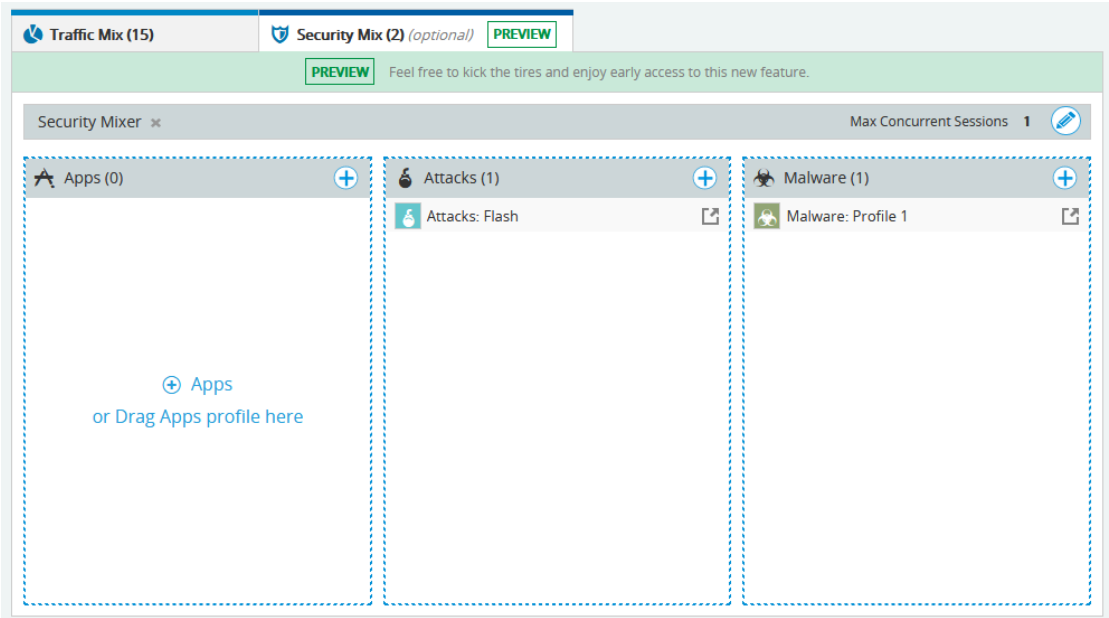



Save Attacks Profile
Scenarios (51)
01 Adobe Flash Player Memory Corruption
02 Adobe Flash Player MP4 File Memory Corruption
03 Adobe Flash Player Shader Memory Corruption
04 Adobe Flash MP3 ID3 Tag Integer Overflow
05 Adobe Flash Player FileReference Type Confusion
06 Adobe Flash Player Rectangle Use After Free
07 Adobe Flash Player FLV Processing Buffer Overflow
Profile Name
Attacks: Flash
Description (Optional)
140
New Attacks Profile
Cancel
Save

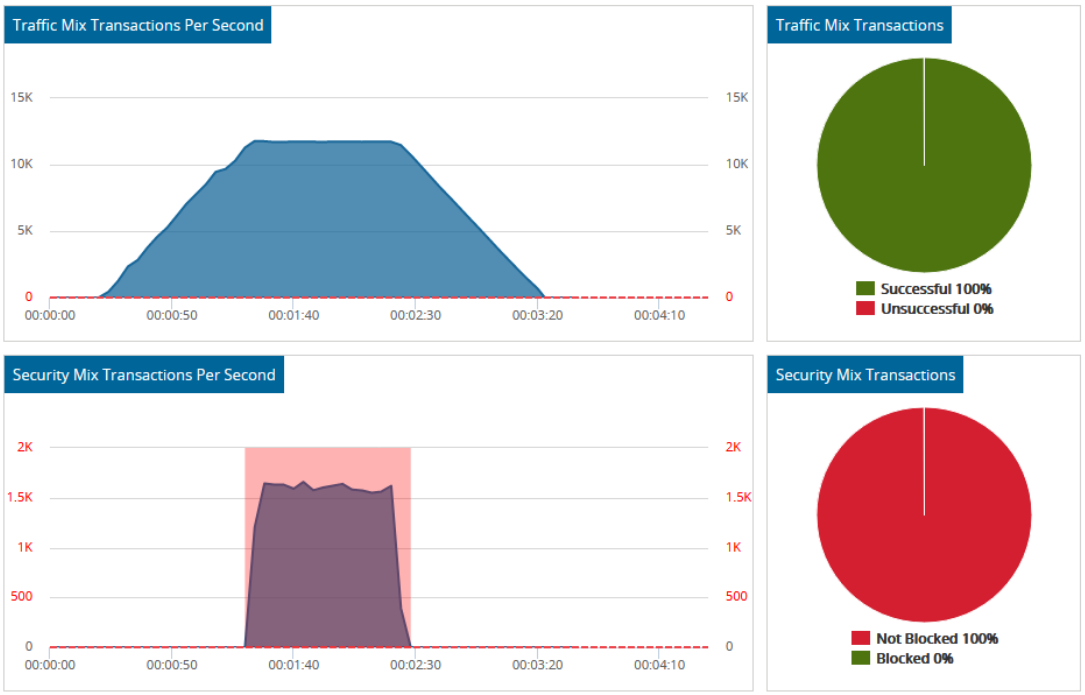
同样的，增加恶意软件。


Create Mix Scenario Profile
Apps
Not Supported
Attacks
Not Supported
Malware
works with
Throughput with Mixed Traffic & CyberSecurity
Cancel
Create Mix Scenario Profile
Import Scenario
773 Found
Add Selected
Add to Profile
Added
Save Malware Profile
Scenarios (2)
01 Trojan-Downloader.Win32.Banload.ykl
02 Trojan.Lineage.Gen.Pac.3
Profile Name
Malware: Profile 1
Description (Optional)
140
New Malware Profile
Cancel
Save
Trojan.Lineage.Gen.Pac.3 is a Trojan application that installs malicious files and libraries on the system and requests malicious
Trojan-Downloader.Win32.Banload.aajs
2 added
Cancel
Save Profile

效果如图。默认最大并发是 1。



运行测试并观察结果。



Security Mix Data

Attacks Data

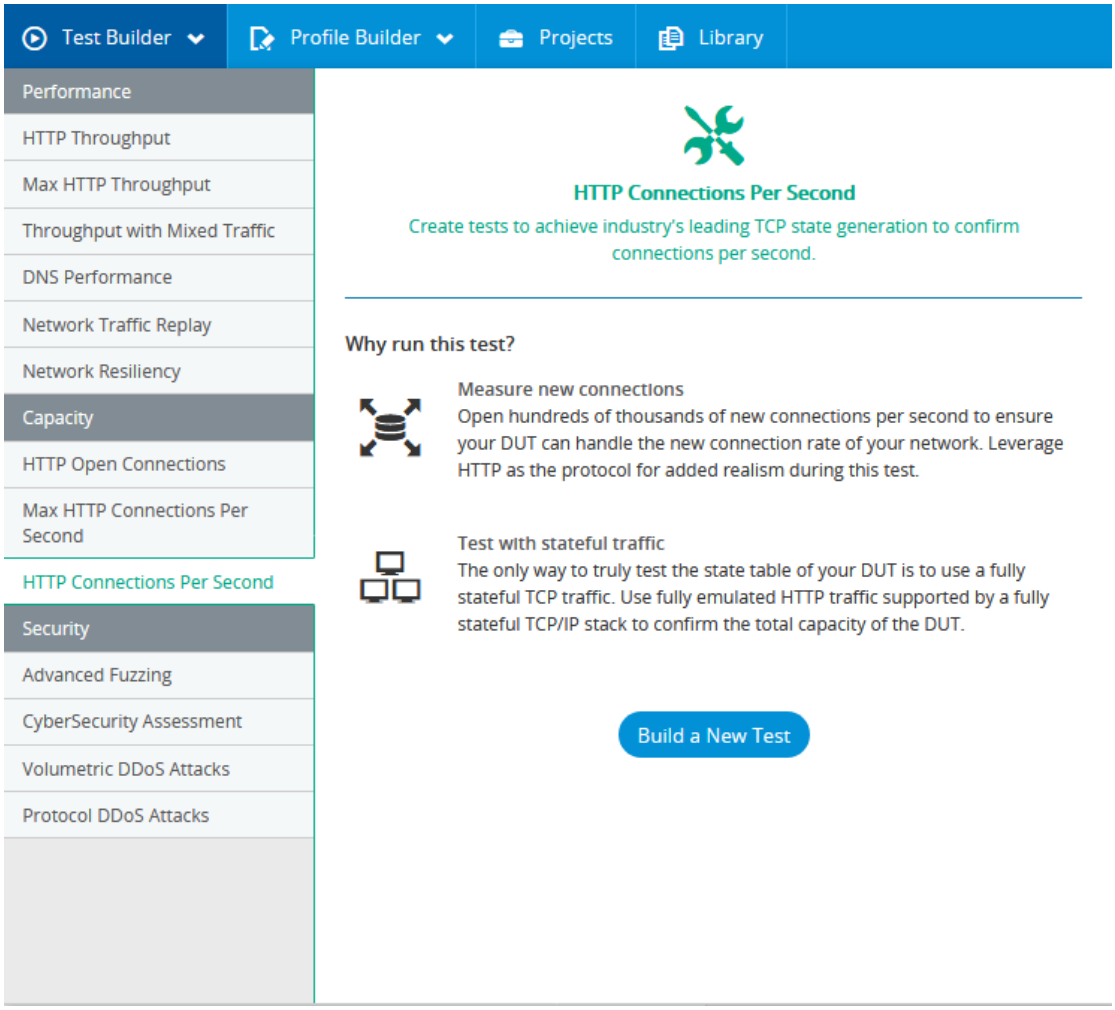
Protocol	Incoming BW	Outgoing BW	Not Blocked Transactions	Blocked Transactions	Attempted Transactions
Attacks: Flash	338.2 Mbps	12.84 Mbps	69 105	0	69 105

Malware Data

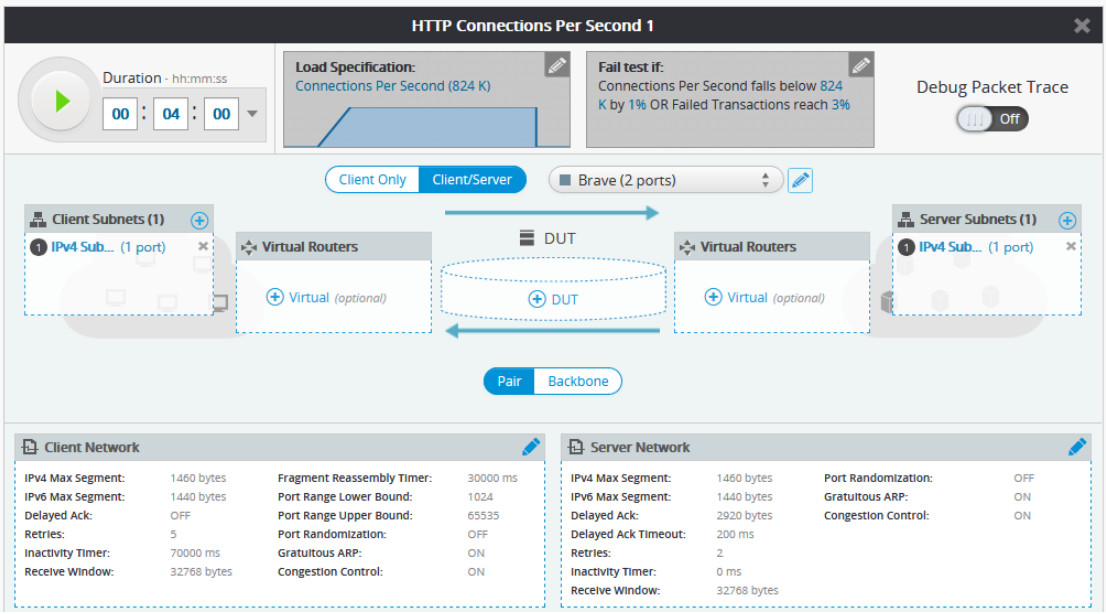
Protocol	Incoming BW	Outgoing BW	Not Blocked Transactions	Blocked Transactions	Attempted Transactions
Malware: Profile 1	620.22 Mbps	13.8 Mbps	27 236	0	27 236

3. HTTP 新建测试

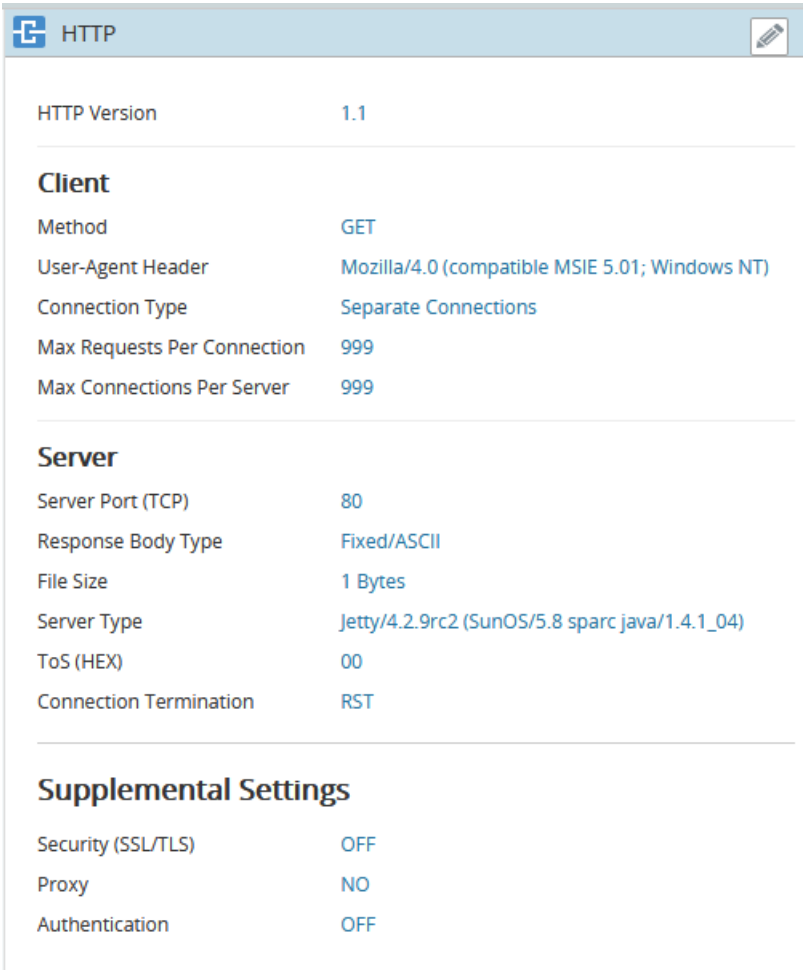
选择 HTTP Connection Per Second 模板，建立测试。



配置测试队列，子网，压力模型。



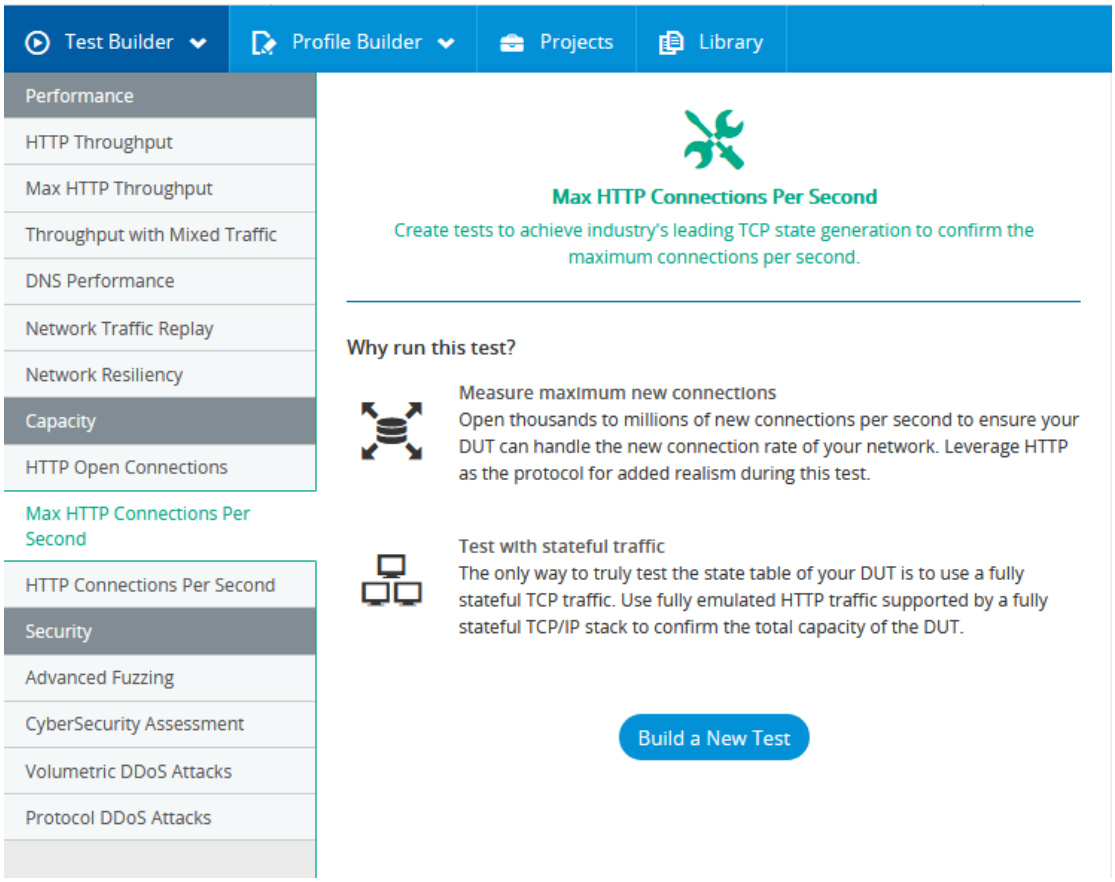
检查或调整 HTTP 层参数。



执行测试。

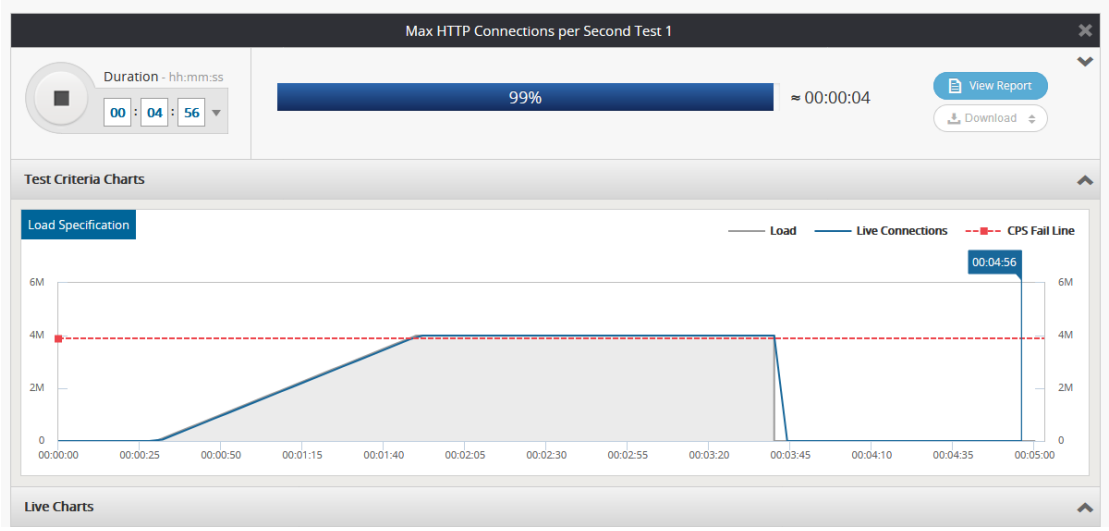
4. 最大 HTTP 新建测试

选择 Max HTTP Connection Per Second 测试模板并建立测试。



配置测试队列，子网，端口等内容。

默认性能为一个核心 100 万新建，根据实际设备的情况调整。
运行测试并观察结果。



5. 网络攻击：Bash 破壳漏洞

Bash 破壳漏洞（Shell Shock）攻击是影响广泛的系统漏洞，CVSS 评分为 10 分，危害性为最高。

Bash 是 Linux 用户广泛使用的一款用于控制命令提示符工具，导致该漏洞影响范围甚广。同时，当 HTTP 服务开放 CGI 服务或其他地方引用 bash 时可直接导致远程命令执行漏洞。主要影响系统为 Readhat、Centos、Ubuntu、Debian、Suse 等主流 Linux 操作系统。

漏洞危害主要表现在：影响基于 bash 开放的服务、程序。当网站利用 CGI 执行 bash 后可导致攻击者远程执行系统命令，从而可以利用系统命令反弹 shell 之后进行内网渗透、挂马、篡改主页、脱库等行为。

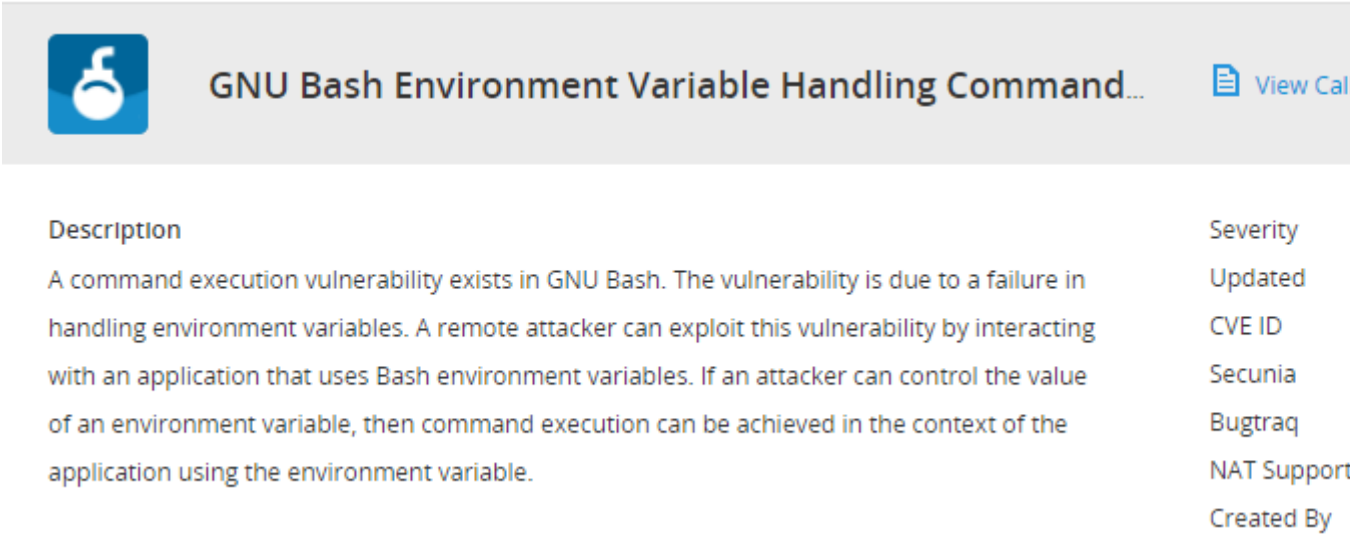
CyberFlood 中 Bash shell shock 的描述

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.

攻击元数据¶

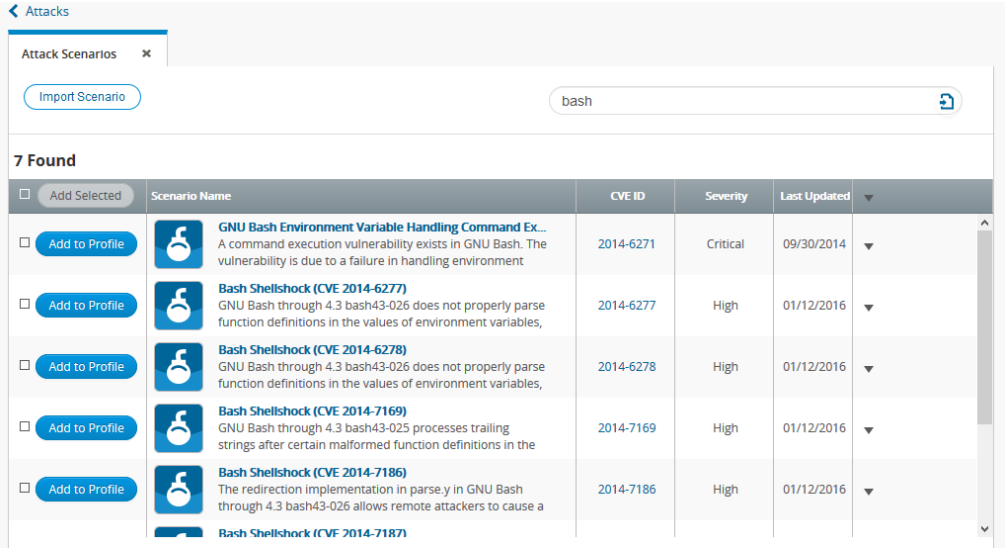
属性	值
Severity	Critical
“CVE ID”	2014-6271

攻击描述

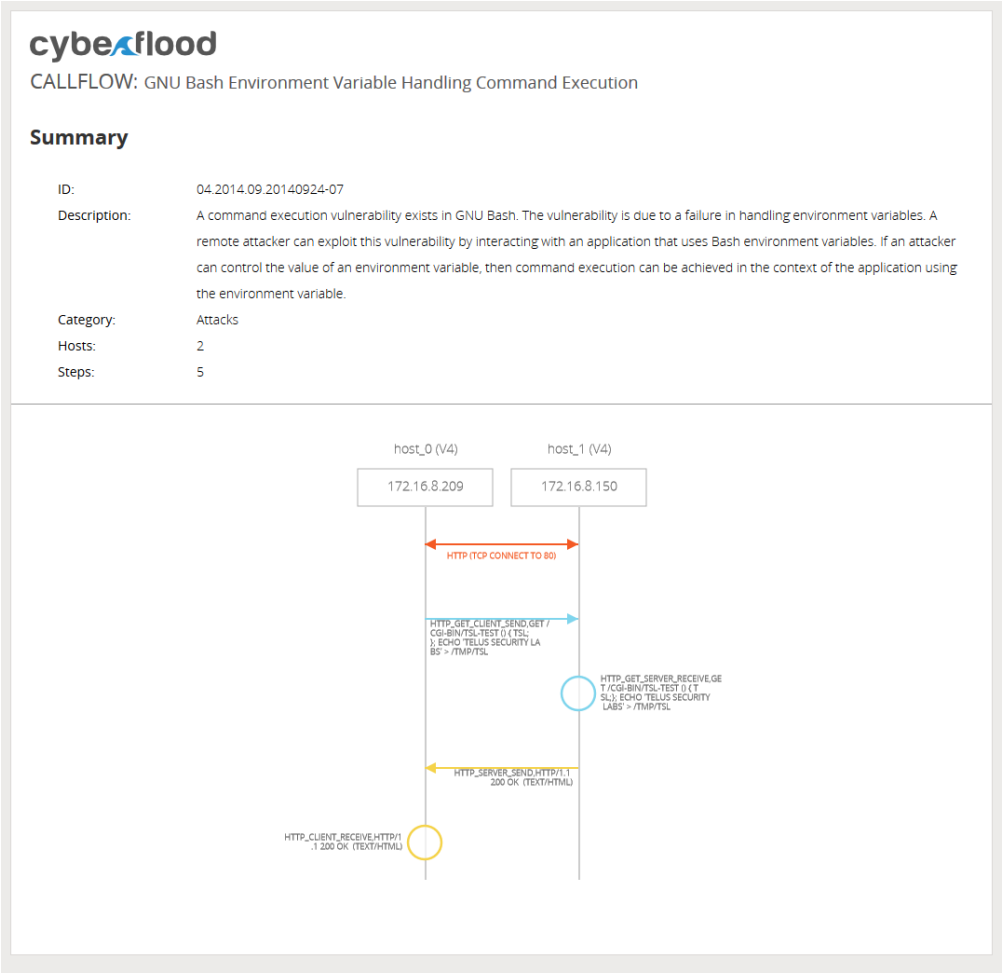


用 CyberFlood 仿真 CVE 2014-6271 攻击

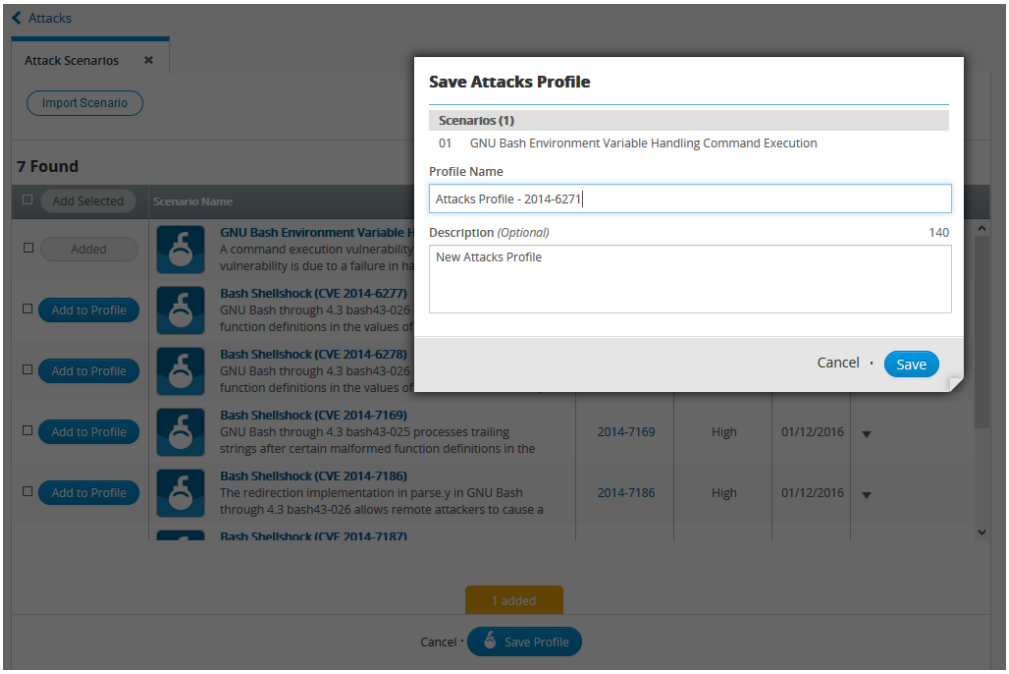
1. 搜索 bash 相关的攻击，找到多个相关漏洞



2. 查看攻击对应的报文流程



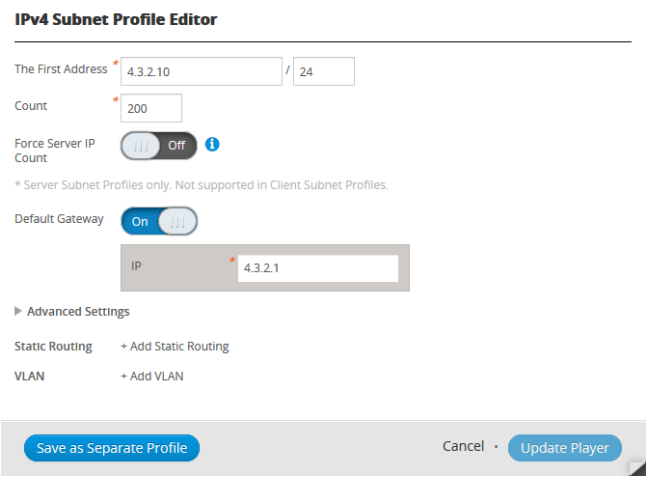
3. 配置 Cyber Security Assessment，发送攻击
    1. ）建议一个攻击 profile。



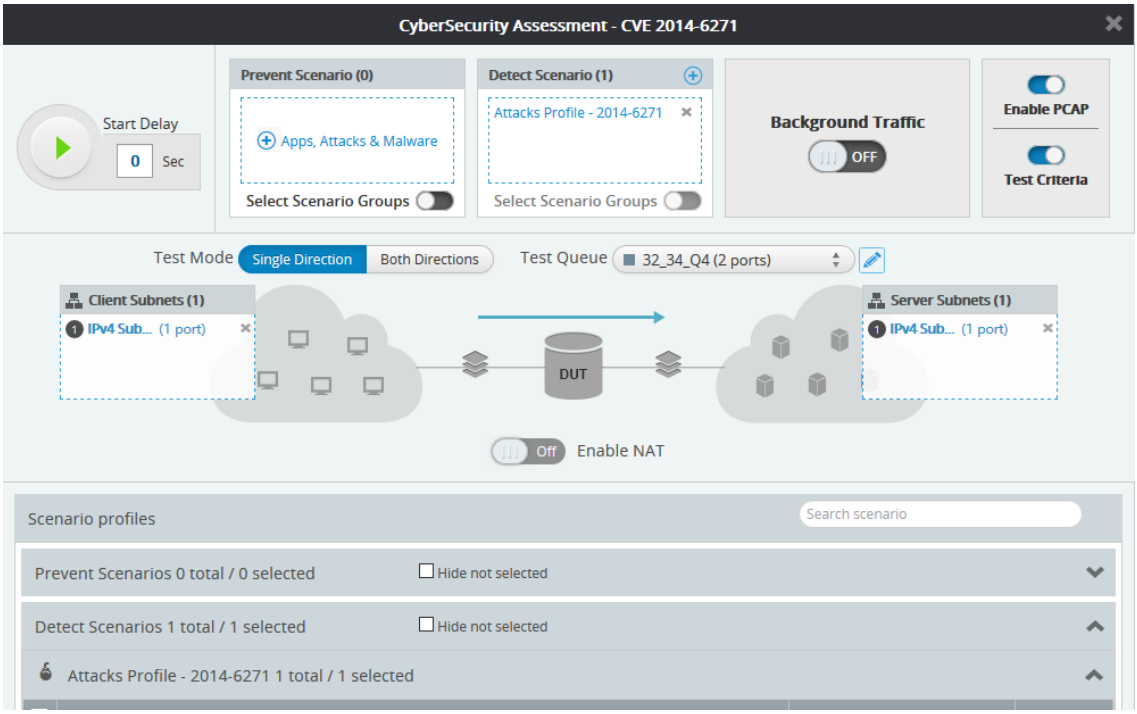
2. ）配置 Cyber Security Assessment。把 *Attack Profile 2014-6271* 从左边拽到右边 detect 模式下。

配置 subnet 和网关。

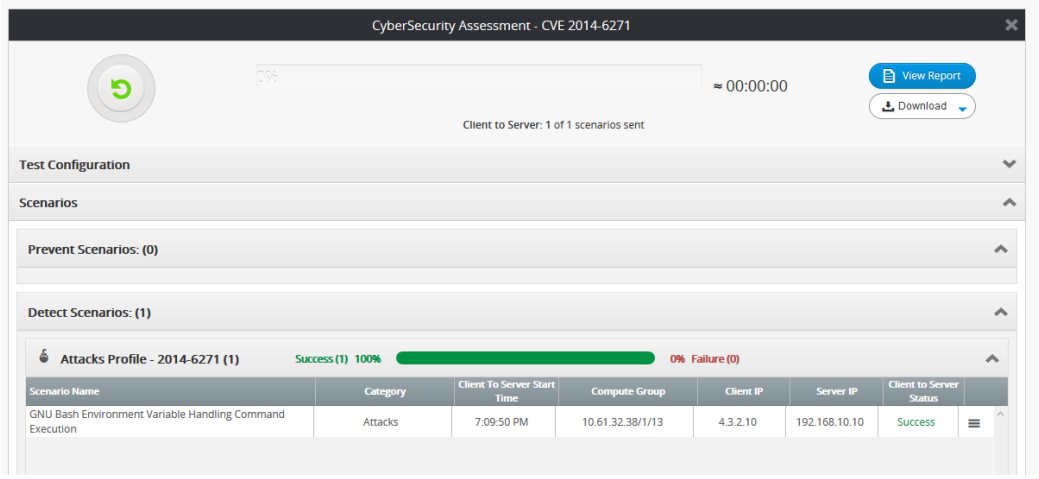
- Client IP 地址范围 4.3.2.10 - 4.3.2.209，网关 4.3.2.1。
- Server IP 地址范围 192.168.10.10 - 192.168.10.209，网关 192.168.10.1。



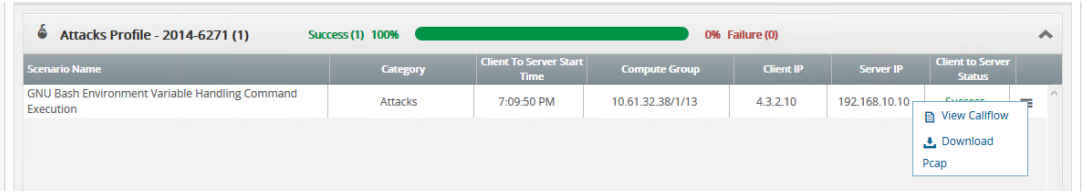
3.）选择队列和端口。打开抓包选项



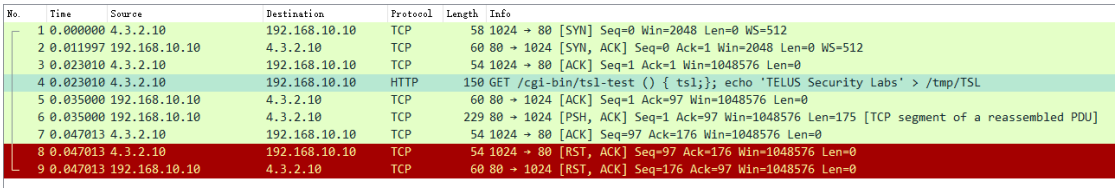
4. ）运行测试，查看结果。



5. ）下载运行时报文。

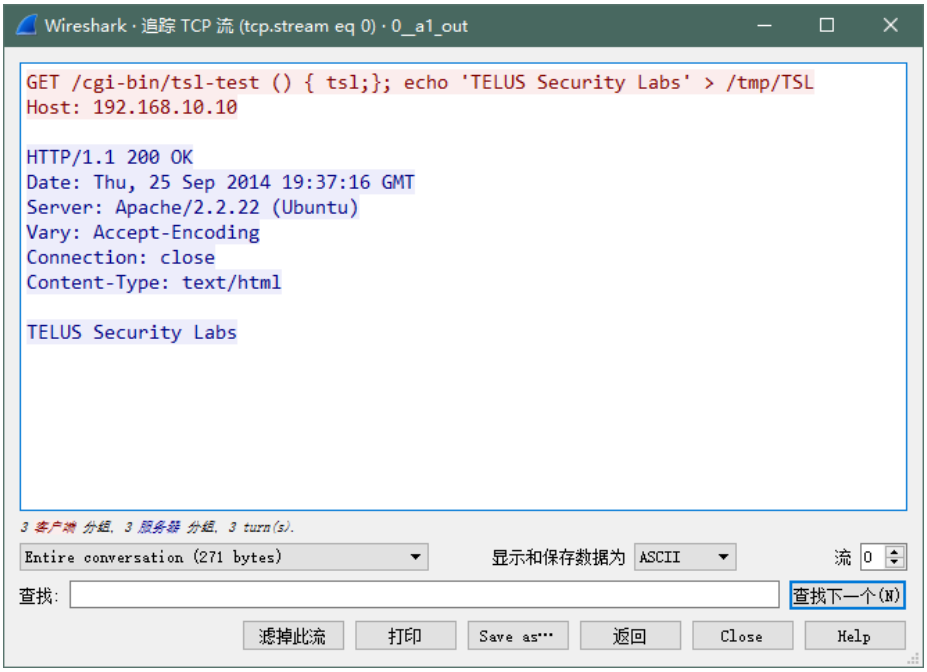


6.）分析报文

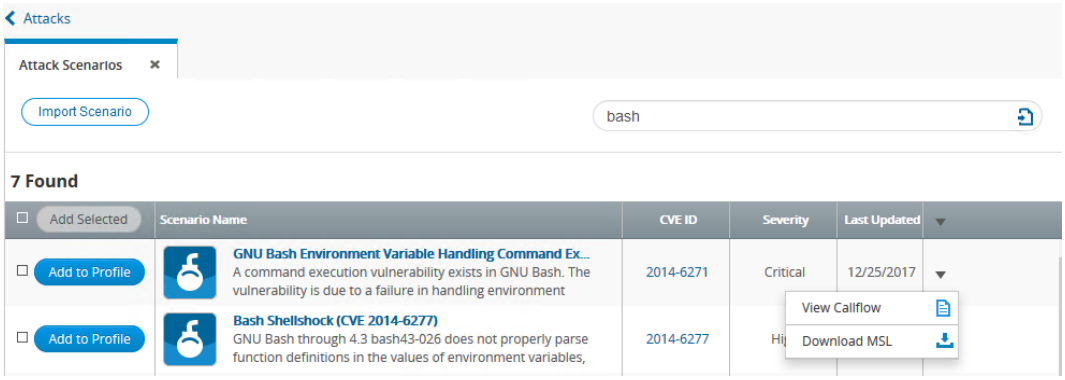


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	4.3.2.10	192.168.10.10	TCP	58	1024 → 80 [SYN] Seq=0 Win=2048 Len=0 WS=512
2	0.011997	192.168.10.10	4.3.2.10	TCP	60	80 → 1024 [SYN, ACK] Seq=0 Ack=1 Win=2048 Len=0 WS=512
3	0.023010	4.3.2.10	192.168.10.10	TCP	54	1024 → 80 [ACK] Seq=1 Ack=1 Win=1048576 Len=0
4	0.023010	4.3.2.10	192.168.10.10	HTTP	150	GET /cgi-bin/ts1-test () { ts1;}; echo 'TELUS Security Labs' > /tmp/TSL
5	0.035000	192.168.10.10	4.3.2.10	TCP	60	80 → 1024 [ACK] Seq=1 Ack=97 Win=1048576 Len=0
6	0.035000	192.168.10.10	4.3.2.10	TCP	229	80 → 1024 [PSH, ACK] Seq=1 Ack=97 Win=1048576 Len=175 [TCP segment of a reassembled PDU]
7	0.047013	4.3.2.10	192.168.10.10	TCP	54	1024 → 80 [ACK] Seq=97 Ack=176 Win=1048576 Len=0
8	0.047013	4.3.2.10	192.168.10.10	TCP	54	1024 → 80 [RST, ACK] Seq=97 Ack=176 Win=1048576 Len=0
9	0.047013	192.168.10.10	4.3.2.10	TCP	60	80 → 1024 [RST, ACK] Seq=176 Ack=97 Win=1048576 Len=0

跟踪一条业务流。注意观察请求的 URL 内容。



7.） 下载并分析报文 msl 文件，查看规则。



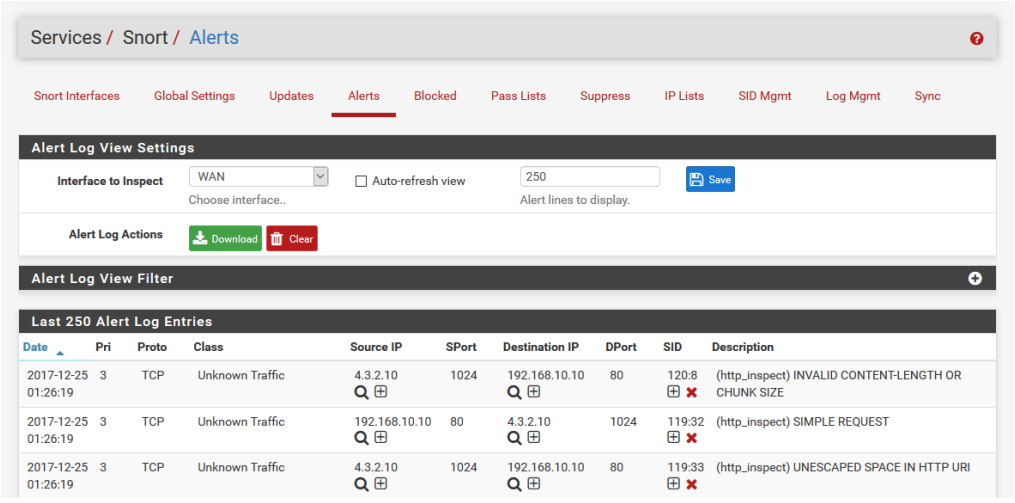
通过文本编辑器打开 msl，查看攻击原理。

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

    # GET /cgi-bin/tsl-test () { tsl;}; echo 'TELUS Security Labs' > /tmp/TSL
    HTTP_GET_Client_Send = HTTP.client_send {
        # http|Hypertext Transfer Protocol
        struct [
            "GET /cgi-bin/tsl-test () { tsl;}; echo \'TELUS Security Labs\' > /tmp/TSL\r\n"
            "Host: #{@HTTP.dst_ip}\r\n"
            "\r\n"
        ]
    }

    # GET /cgi-bin/tsl-test () { tsl;}; echo 'TELUS Security Labs' > /tmp/TSL
    HTTP_GET_Server_Receive = HTTP_GET_Client_Send.server_receive

    # HTTP/1.1 200 OK  (text/html)
    HTTP_Server_Send = HTTP.server_send {
        # http|Hypertext Transfer Protocol
        struct [
            "HTTP/1.1 200 OK\r\n"
            "Date: Thu, 25 Sep 2014 19:37:16 GMT\r\n"
            "Server: Apache/2.2.22 (Ubuntu)\r\n"
            "Vary: Accept-Encoding\r\n"
            "Connection: close\r\n"
            "Content-Type: text/html\r\n"
            "\r\n"
            content_1 = "TELUS Security Labs\n"
        ]
    }
```

2. 观察 snort 防火墙的告警

PfSense 可以安装 snort 防火墙。通过 Services -> Snort -> Alerts 查看 Snort 的安全日志。可以看到 snort 的告警为 *UNESCAPED SPACE IN HTTP URI* 和 *INVALID CONENTE-LENGTH OR CHUNK SIZE* 。

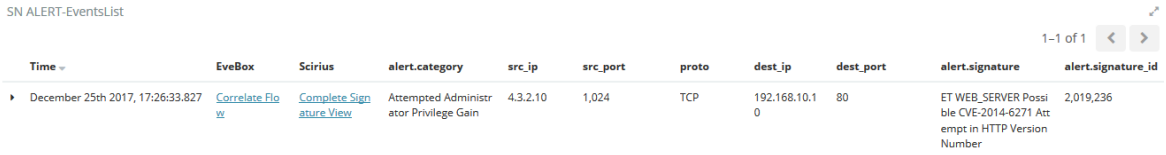
可以看出 snort 并没有检测出这个攻击。属于漏报攻击。对于靶场，这是一个很好的素材，需要认真分析规则库的内容，判断是规则没有更新还是规则的内容无法识别该攻击。



3. 观察 suricata 的告警

我们使用了 SELKS 内置的 suricata，版本是 4.0.0。

1.）通过 SELKS 的 Kibana 看到一条安全日志，显示源 IP 是 4.3.2.10，目的 IP 是 192.168.10.10，目的端口是 80。告警的签名是 *ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Version Number*


SN ALERT-EventsList

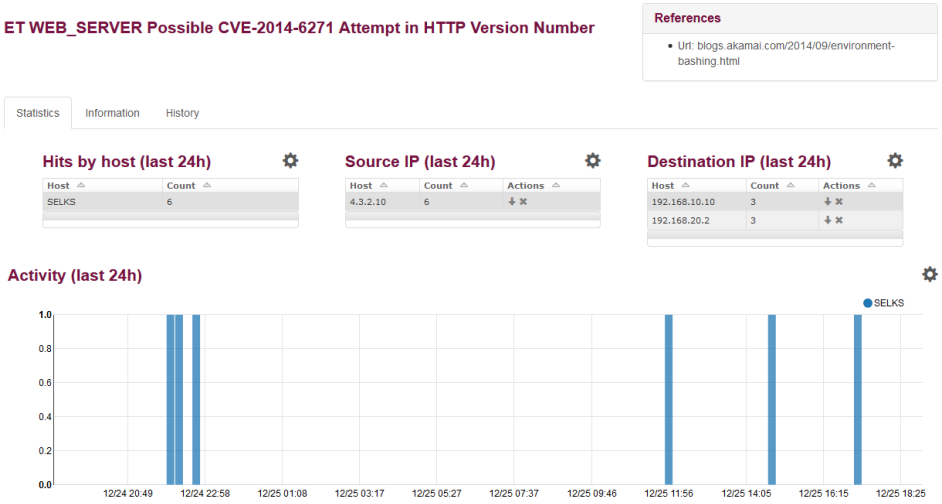
1–1 of 1

Time	EveBox	Scirius	alert.category	src_ip	src_port	proto	dest_ip	dest_port	alert.signature	alert.signature_id
December 25th 2017, 17:26:33.827	Correlate Flow	Complete Signature View	Attempted Administrator Privilege Gain	4.3.2.10	1,024	TCP	192.168.10.10	80	ET WEB_SERVER Possible CVE-2014-6271 Attempt in HTTP Version Number	2,019,236

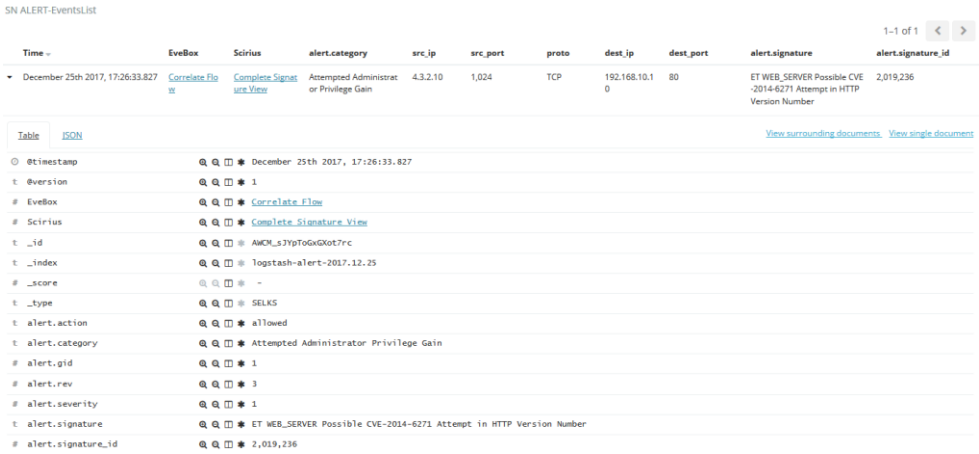
2.）点击 *Complete Signature View* 查看具体触发了那条规则。

3.）通过分析，这条规则检查内容中的 *| 20 28 29 20 7b|*。这是 suricata 语法，即检查 raw_bytes。 这 5 个字节对应 *“ () {“*。

4.） 点击 Statistics，查看该规则的统计。规则在 24 号和 25 号都触发过，这是因为我们反复用这条攻击做测试。在实战中如果某一规则反复触发，需要特别引起关注。



5.） 再回到 Kibana，看一下 Suricata 的规则和对应抓取到的报文。



http_method 是 GET，payload_printable 的内容触发了规则。

可以看出 Suricata 很好的识别了 CVE 2014-6271 破壳漏洞攻击，告警信息正确，完备。