

H3C SecPath M9000 测试报告



H3C SecPath M9000 测试报告

Table of Contents

测试报告综述	1
测试结果亮点	1
测试设备说明	2
被测设备	2
测试仪表	2
测试辅助设备	2
测试组网说明	3
网络层性能测试组网	3
应用层性能测试组网	3
可靠性测试组网	4
测试用例及结果快速索引	4
测试用例和结果汇总	6
320G 单板网络层防火墙吞吐性能测试	6
整机 1.92T 网络层防火墙吞吐性能测试	8
320G 单板应用层防火墙处理性能测试	10
100G 业务板单板网络层防火墙吞吐性能测试	15
100G 业务板单板应用层防火墙叠加处理性能测试	16
虚拟防火墙功能验证测试	18
网络特征攻防测试	21
防火墙 HA 可靠性测试	24

H3C SecPath M9000 测试报告

测试报告综述

H3C SecPath M9000 系列是新华三集团结合云计算、IPv6、大数据及高性能计算的发展趋势，在大安全领域针对云计算数据中心、运营商 CGN、大型企业及园区网出口等市场推出的新一代高性能多业务安全网关。

此次采用思博伦专业性能和安全测试仪表和测试方法评测新华三防火墙业务板的处理能力，为通过测试突出反映 H3C SecPath M9000 系列超高端防火墙业务板在真实网络模拟环境下的最佳性能表现，为该产品提供最有利的技术和质量评估。

本测试采用了 RFC3511 和 RFC2544 的性能测试方法，对 SecBlade IV 320G 防火墙业务板模块和 SecBlade IV 100G 防火墙业务板模块进行了测试。

测试结果亮点

- ✓ SecBlade IV 320G 防火墙业务板单板性能
 - 网络层防火墙吞吐处理能力 高达 317.7 Gbps;
 - 可支持 HTTP 每秒新建连接数 (CPS) 达到 795,000;
 - 可支持 HTTP 并发连接数 达到 81,600,000;
- ✓ SecBlade IV 100G 防火墙业务板单板性能
 - 网络层防火墙吞吐处理能力 线速 100Gbps;
 - 应用层 HTTP 叠加性能处理能力，可同时满足 100G 应用层线速吞吐 + 400,000 每秒新建 TCP 连接 + 16,000,000 TCP 并发连接保持，并保持长时间稳定工作；
- ✓ M9014 1.92T 规格整机网络层防火墙吞吐处理能力 高达 1.84 Tbps;
- ✓ IPv6 业务性能与 IPv4 业务性能对比无明显差异；
- ✓ 防火墙网络安全攻防能力强，主流攻击漏洞采样下的阻挡率评级为 A；
- ✓ M9014 虚拟防火墙功能切实有效；虚墙独立重起不影响其它虚墙正常运行；虚拟防火墙的吞吐量、会话新建速率等资源可实现动态调整；
- ✓ M9014 各种冗余设计可靠性切实有效；可实现主-备、主-主模式双机热备；

H3C SecPath M9000 测试报告

测试设备说明

被测设备

被测试设备选用 H3C SecPath M9014 两台。每台 M9014 必配主控制模块 2 块，交换引擎 4 块。每台 M9014 配备如下业务板以用于测试需要：

- SecBlade IV 320G 防火墙业务板 (H3C NSQM1FWDFG0)
- SecBlade IV 100G 防火墙业务板 (H3C NSQM1FWDFGD1)
- 32 端口万兆以太网光接口模块 (H3C NSQ1TGS32SF0)
- 2 端口 100G 以太网光接口板 (H3C NSQ1CGC2SE0)

测试仪表

网络层测试方案选用思博伦公司的 Spirent Test Center N11U 机框和 DX2 Test Modules，具体测试模块物料如下：

- 32 端口万兆以太网测试模块(DX2-10G-Q8)（整机测试使用 6 块该模块）

应用层测试方案选用思博伦公司的 Spirent C100-S3-MP 系列仪表，具体物料如下：

- Spirent C100-S3-MP 一台， 2 x 100G 光测试端口模式 (QSFP28)
- Spirent C100-S3-MP 一台， 8 x 10G 光测试端口模式 (SFP+)

测试辅助设备

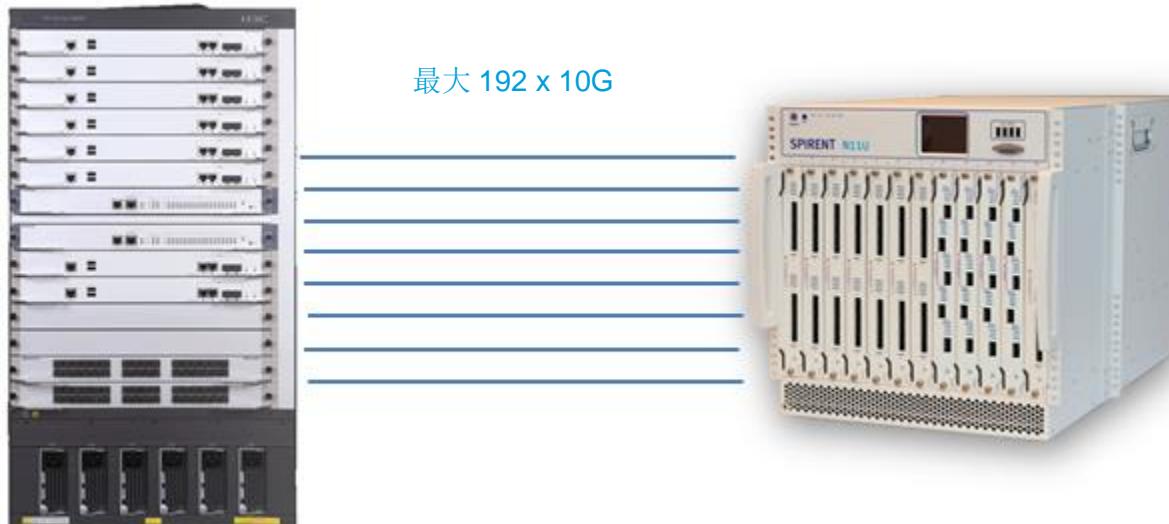
- Windows 操作系统 PC 一台
 - 用于安装 Spirent TestCenter Application 测试软件 (ver 4.66 版本)
 - 用于安装 Spirent Avalanche Commander 测试软件 (ver 4.66 版本)
- VMWare ESXi 服务器提供如下系统资源
 - CPU: 2+ GHz Dual Core (64-bit)
 - 内存: 不低于 8GB 内存
 - 磁盘: 不低于 128GB

以上资源用于部署 Spirent CyberFlood™ Controller 虚拟机一台 (ver 16.4.0 版本)

H3C SecPath M9000 测试报告

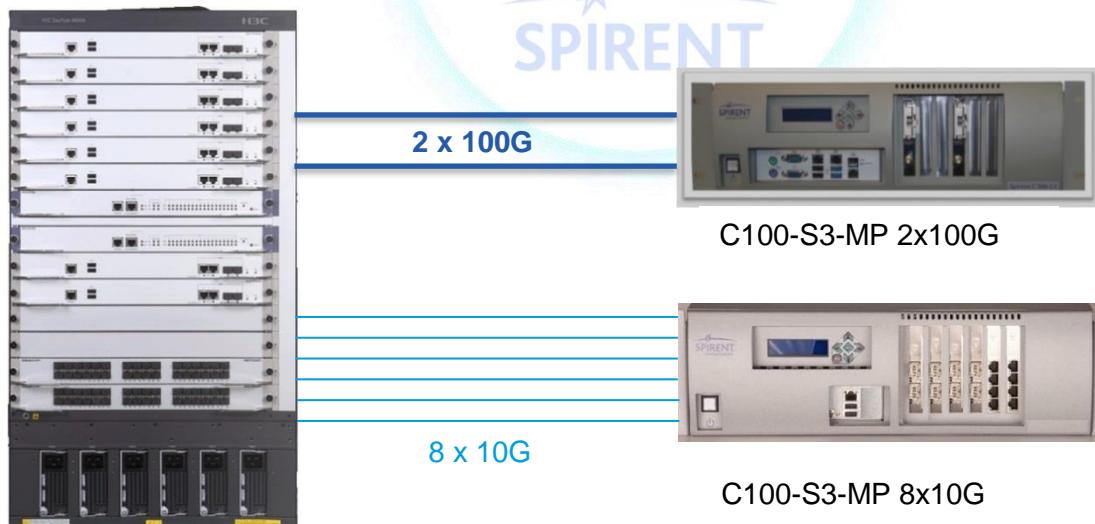
测试组网说明

网络层性能测试组网



H3C SecPath M9014

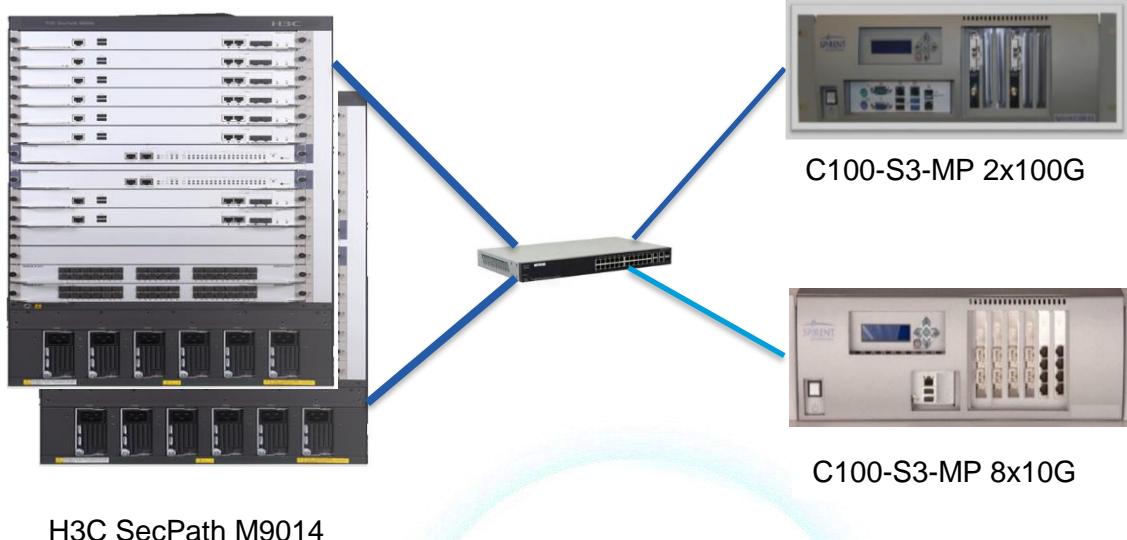
应用层性能测试组网



H3C SecPath M9014

H3C SecPath M9000 测试报告

可靠性测试组网



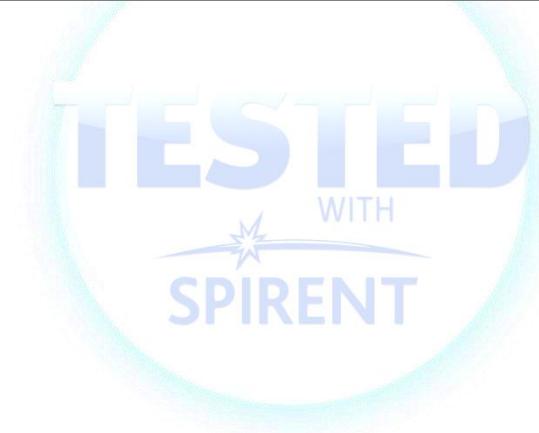
测试用例及结果快速索引

下表总结了各项测试内容和测试结果，点击相应条目可以跳转到相应的测试方案章节。

测试类别	测试用例	测试主结果
<u>320G 业务板单板网络层防火墙吞吐性能</u>	IPv4 UDP 流量网络吞吐性能(单板)	317.7 Gbps
	IPv6 UDP 流量网络吞吐性能(单板)	317.7 Gbps
<u>1.92T 整机网络层防火墙吞吐性能</u>	IPv4 UDP 流量网络吞吐性能(整机)	1.85 Tbps
	IPv6 UDP 流量网络吞吐性能(整机)	1.7 Tbps
<u>320G 业务板单板应用层防火墙性能</u>	IPv4 TCP 最大新建连接速率	795,000
	IPv6 TCP 最大新建连接速率	794,000
	IPv4 TCP 最大并发保持数	81,600,000
	IPv6 TCP 最大并发保持数	81,600,000

H3C SecPath M9000 测试报告

<u>100G 业务板单板网络层防火墙吞吐性能</u>	IPv4 UDP 流量网络吞吐性能(单板)	100 Gbps
<u>100G 业务板单板应用层防火墙叠加处理性能</u>	IPv4 应用叠加处理性能(单板)	100 Gbps + 160,000 每秒新建连接 + 60,000,000 并发连接保持
<u>虚拟防火墙功能验证测试</u>	虚墙重启功能验证	通过
	虚墙动态资源分配验证	通过
<u>特性攻防测试</u>	最新攻击样本扫描检测	A
<u>HA 可靠性测试</u>	单机故障模拟下业务状态监测	通过
	HA 双机故障模拟下业务状态监测	通过



H3C SecPath M9000 测试报告

测试用例和结果汇总

320G 单板网络层防火墙吞吐性能测试

测试描述	
ID	T_NETPERF_320G_UDP_IPv4
描述	
描述	通过仪表的 32 个 10GE 接口，连接被测试设备的接口板，配置仪表产生 IPv4 UDP 流量，运行 RFC2544 测试基准，测试 UDP 转发吞吐量及时延特性。
测试执行参数	
测试执行参数	<ul style="list-style-type: none">■ 配置 32 端口的 Full Mesh 流量■ 报文内容为 IPv4 UDP■ 测试使用端口：32*10GE
测试指标关注	
测试指标关注	<ul style="list-style-type: none">■ RFC2544 测试基准■ 记录报告中的吞吐量及时延值

下表列出了防火墙 320G 单板采用 RFC2544 测试方法实测得到的 IPv4 UDP 报文在不同帧长下网络吞吐性能和网络延迟结果。

帧长(字节)	66	128	256	512	1024	1280	1518
最大 fps	121M	119M	106M	67M	38M	30.5M	26M
最大吞吐(Gbps)	83.7	142	234	286	315	317.7	317.7
平均延时(uSec)	8.76	8.71	9.37	9.91	12	13.44	19.6
Frame 丢包率	0%	0%	0%	0%	0%	0%	0%

其中，可获得的最大吞吐为 317.7 Gbps，达到理论吞吐上限的 99.3%。

H3C SecPath M9000 测试报告

测试描述	
ID	T_NETPERF_320G_UDP_IPv6
描述	
描述	通过仪表的 32 个 10GE 接口，连接被测试设备的接口板，配置仪表产生 IPv6 UDP 流量，运行 RFC2544 测试基准，测试 UDP 吞吐量及时延特性。
测试执行参数	
测试执行参数	<ul style="list-style-type: none">■ 配置 32 端口的 Full Mesh 流量■ 报文内容为 IPv6 UDP■ 测试使用端口：32*10GE
测试指标关注	<ul style="list-style-type: none">■ RFC2544 测试基准■ 记录报告中的吞吐量及时延值

下表列出了防火墙 320G 单板采用 RFC2544 测试方法实测得到的 IPv6 UDP 报文在不同帧长下网络吞吐性能和网络延迟结果。

帧长(字节)	86	128	256	512	1024	1280	1518
最大 fps	119M	119M	106M	67M	38M	30.5M	26M
最大吞吐(Gbps)	101.7	142	234	286	315	317.7	317.7
平均延时(uSec)	8.53	8.62	9.2	10.7	15.54	18.63	20.74
Frame 丢包率	0%	0%	0%	0%	0%	0%	0%

其中，可获得的最大吞吐为 317.7 Gbps，达到理论吞吐上限的 99.3%。

H3C SecPath M9000 测试报告

整机 1.92T 网络层防火墙吞吐性能测试

测试描述	
ID	T_NETPERF_1_92T_UDP_IPv4
描述	通过仪表的 192 个 10GE 接口，连接被测试设备的满配置的所有接口板，配置仪表产生 IPv4 UDP 流量，运行 RFC2544 测试基准，测试 UDP 吞吐量及时延特性。
测试执行参数	
测试执行参数	<ul style="list-style-type: none">■ 配置 192 端口的 Full Mesh 流量■ 报文内容为 IPv4 UDP■ 测试使用端口：192*10GE
测试指标关注	<ul style="list-style-type: none">■ RFC2544 测试基准■ 记录报告中的吞吐量及时延值

下表列出了防火墙整机采用 RFC2544 测试方法实测得到 IPv4 UDP 报文在不同帧长下网络吞吐性能和网络延迟结果。

帧长(字节)	66	128	256	512	1024	1280	1518
最大 fps	690M	698M	612M	387M	220M	176M	150M
最大吞吐(Gbps)	475.5	826.5	1353	1650	1839	1839	1852
平均延时(uSec)	9.19	9.58	10.10	10.24	16.56	17.67	19.49
Frame 丢包率	0%	0%	0%	0%	0%	0%	0%

其中，可获得的最大吞吐为 1852 Gbps，达到理论吞吐上限的 96.5%。

H3C SecPath M9000 测试报告

测试描述	
ID	T_NETPERF_1_92T_UDP_IPv6
描述	通过仪表的 192 个 10GE 接口，连接被测试设备满配置的所有接口板，配置仪表产生 IPv6 UDP 流量，运行 RFC2544 测试基准，测试 UDP 吞吐量及时延特性。
测试执行参数	
测试执行参数	<ul style="list-style-type: none">■ 配置 192 端口的 Full Mesh 流量■ 报文内容为 IPv6 UDP■ 测试使用端口：192*10GE
测试指标关注	<ul style="list-style-type: none">■ RFC2544 测试基准■ 记录报告中的吞吐量及时延值

下表列出了防火墙整机采用 RFC2544 测试方法实测得到 IPv6 UDP 报文在不同帧长下网络吞吐性能和网络延迟。

帧长(字节)	86	128	256	512	1024	1280	1518
最大 fps	683M	674M	606M	384M	202M	164M	138M
最大吞吐(Gbps)	583.5	799.5	1339.5	1636.5	1690.5	1704	1704
平均延时(uSec)	10.37	9.9	10.14	11.25	13.86	16.02	17.48
Frame 丢包率	0%	0%	0%	0%	0%	0%	0%

其中，可获得的最大吞吐为 1704 Gbps，达到理论吞吐上限的 88.7%。

H3C SecPath M9000 测试报告

320G 单板应用层防火墙处理性能测试

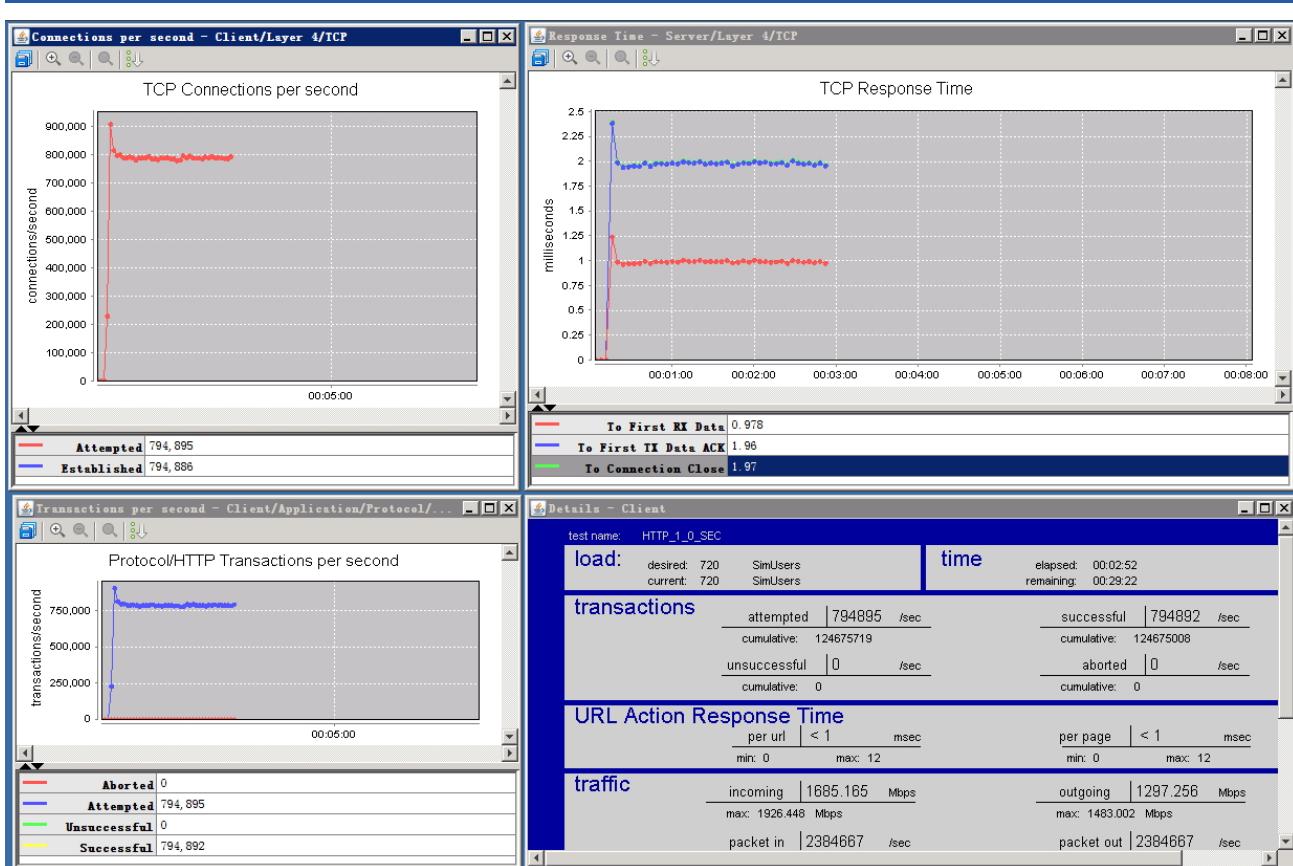
IPv4 TCP 最大新建速率

测试描述	
ID	T_PERF_320G_CPS_IPV4
描述	
描述	通过仪表双臂部署模拟客户端和服务器，测试寻找到满配测试端口情况下防火墙业务单板能够支持的 IPv4 TCP 连接建立的最大速率。
测试执行参数	
测试执行参数	<ul style="list-style-type: none">■ IP 版本: IPv4■ 测试协议: HTTP / TCP■ 测试使用端口: 2 x 100G■ 压力模型: Connection per second
测试指标关注	<ul style="list-style-type: none">■ TCP Connection Per Second■ TCP Response Time■ Total Failure Transactions

下表列出了实测结果。

指标	结果
TCP Connection Per Second	795,000
TCP Response Time (To first Rx data)	0.98 millisecond
Total Failure Transactions	0

H3C SecPath M9000 测试报告



IPv6 TCP 最大新建速率



测试描述

ID	T_PERF_320G_CPS_IPV6
描述	通过仪表双臂部署模拟客户端和服务器，测试寻找到满配测试端口情况下防火墙业务单板能够支持的 IPv6 TCP 连接建立的最大速率。

测试执行参数

测试执行参数	<ul style="list-style-type: none">IP 版本: IPv6测试协议: HTTP / TCP测试使用端口: 2 x 100G压力模型: Connection per second
--------	---

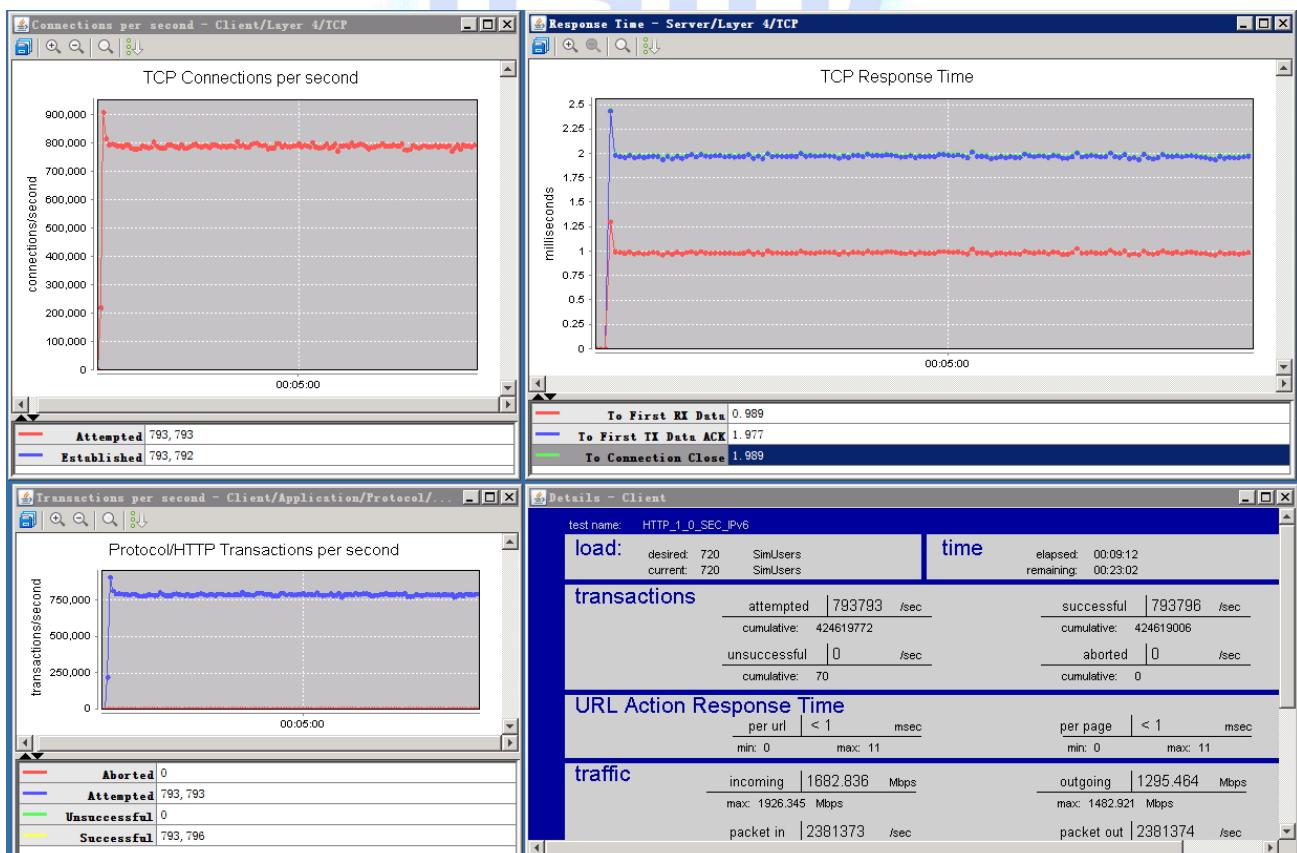
H3C SecPath M9000 测试报告

测试指标关注

- TCP Connection Per Second
- TCP Response Time
- Total Failure Transactions

下表列出了实测结果。

指标	结果
TCP Connection Per Second	794,000
TCP Response Time (To first Rx data)	0.98 millisecond
Total Failure Transactions	0



H3C SecPath M9000 测试报告

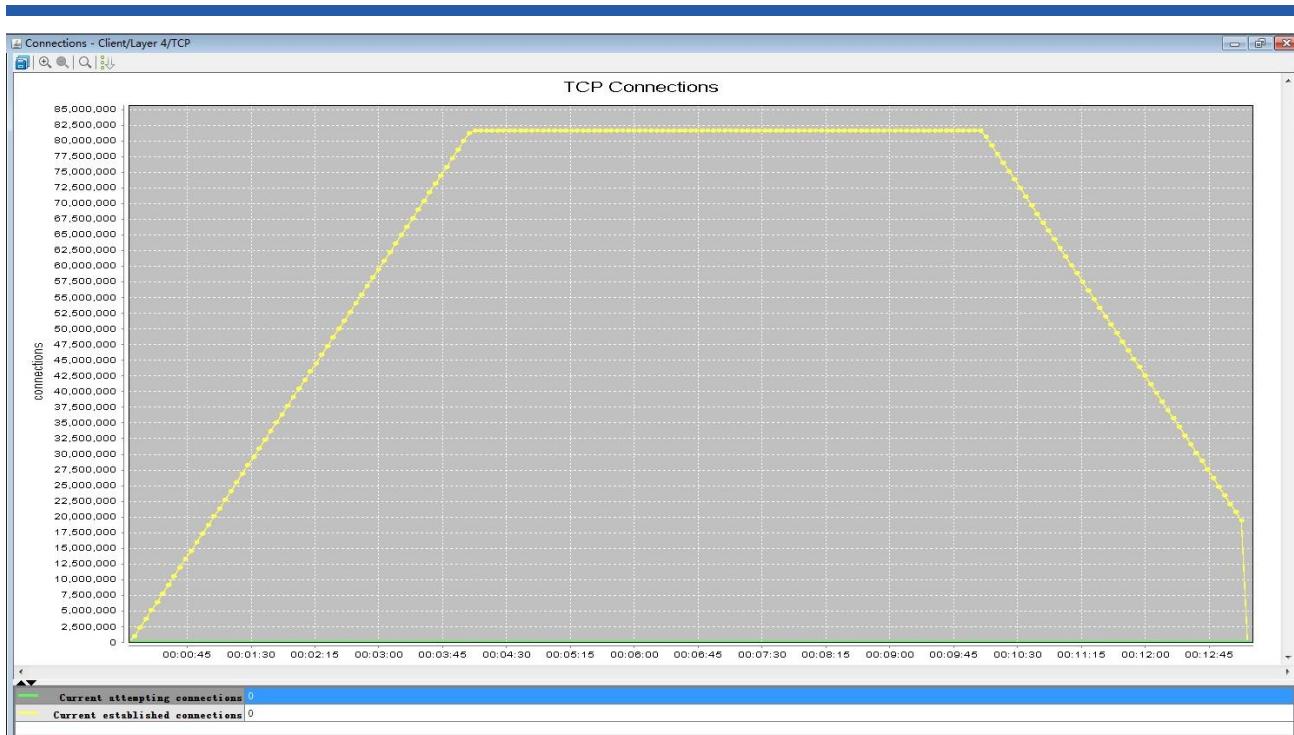
IPv4 TCP 最大并发数

测试描述	
ID	T_PERF_320G_CCS_IPV4
描述	
描述	通过仪表双臂部署模拟客户端和服务器，测试寻找到满配测试端口情况下防火墙业务单板能够支持的 IPv4 TCP 同时连接的最大数量。
测试执行参数	
测试执行参数	<ul style="list-style-type: none">■ IP 版本: IPv4■ 测试协议: HTTP / TCP■ 测试使用端口: 2 x 100G■ 压力模型: SimUser
测试指标关注	<ul style="list-style-type: none">■ TCP Current Connections■ Total Failure Transactions

下表列出了实测结果。

指标	结果
TCP Concurrent Connections	81,600,000
Total Failure Transactions	0

H3C SecPath M9000 测试报告



IPv6 TCP 最大并发数

TESTED

测试描述

ID	T_PERF_320G_CCS_IPV6
描述	通过仪表双臂部署模拟客户端和服务端，测试寻找到满配测试端口情况下防火墙业务单板能够支持的 IPv6 TCP 同时连接的最大数量。

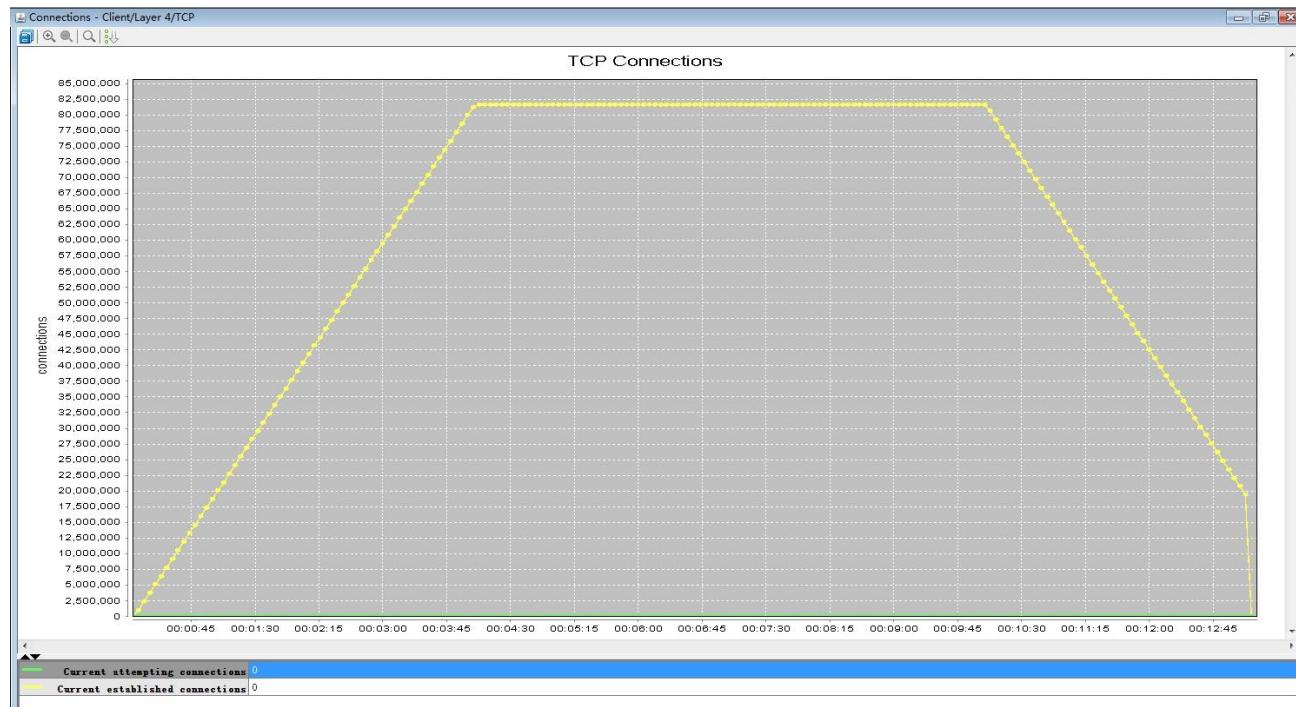
测试执行参数

测试执行参数	<ul style="list-style-type: none">■ IP 版本: IPv6■ 测试协议: HTTP / TCP■ 测试使用端口: 2 x 100G■ 压力模型: SimUser
测试指标关注	<ul style="list-style-type: none">■ TCP Current Connections■ Total Failure Transactions

H3C SecPath M9000 测试报告

下表列出了实测结果。

指标	结果
TCP Concurrent Connections	81,600,000
Total Failure Transactions	0



100G 业务板单板网络层防火墙吞吐性能测试

测试描述	
ID	T_NETPERF_100G_UDP_IPv4
描述	通过仪表的 10 个 10GE 接口，连接被测试设备的接口板，配置仪表产生 IPv4 UDP 流量，运行 RFC2544 测试基准，测试 UDP 转发吞吐量及时延特性。
测试执行参数	

H3C SecPath M9000 测试报告

测试执行参数	<ul style="list-style-type: none">■ 配置 10 端口的 Full Mesh 流量■ 报文内容为 IPv4 UDP■ 测试使用端口: 10 * 10GE
测试指标关注	<ul style="list-style-type: none">■ RFC2544 测试基准■ 记录报告中的吞吐量及延时

下表列出了防火墙 100G 单板采用 RFC2544 测试方法实测得到的 IPv4 UDP 报文在不同帧长下网络吞吐性能和网络延迟结果。

帧长(字节)	66	128	256	512	1024	1280	1518
最大 fps	52.3M	51.8M	45.3M	23.5M	12M	9.6M	8.1M
最大吞吐(Gbps)	36	61.3	100	100	100	100	100
平均延时(uSec)	8.77	8.85	9.92	9.95	11.95	13.01	13.94
Frame 丢包率	0%	0%	0%	0%	0%	0%	0%

其中，可获得的最大吞吐为线速 100 Gbps，达到理论吞吐上限的 100%。

100G 业务板单板应用层防火墙叠加处理性能测试

IPv4 HTTP 应用叠加处理性能

测试描述	
ID	T_PERF_100G_COMBINE_IPV4
描述	通过仪表双臂部署模拟客户端和服务器，在应用层吞吐达到设备线速 100Gbps 的基础上，维持一定规模的 HTTP 新建连接数和 HTTP 并发连接保持数，以模拟实际网络中更为真实的压力条件，

H3C SecPath M9000 测试报告

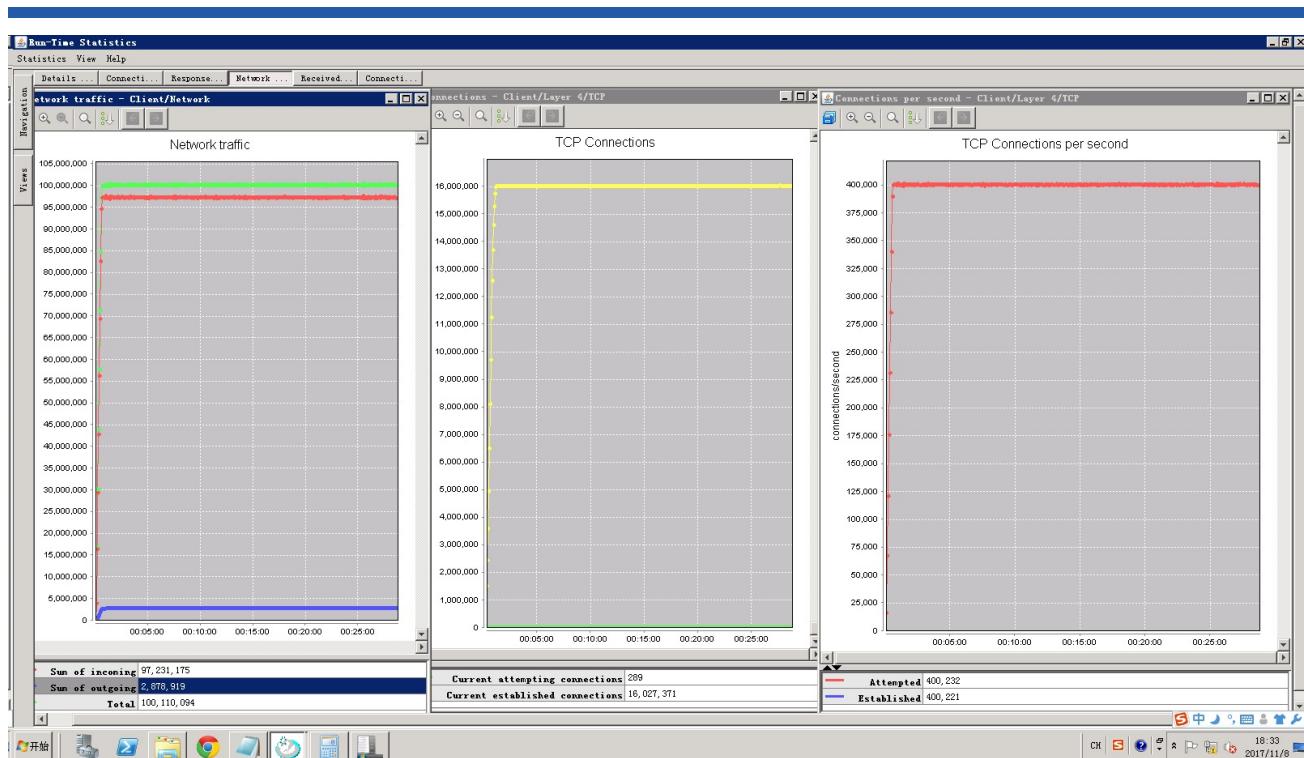
	判断防火墙业务单板是否能够稳定支撑。
测试执行参数	
测试执行参数	<ul style="list-style-type: none">■ IP 版本: IPv4■ 测试协议: HTTP / TCP■ 测试使用端口: 2 x 100G + 8 x 10G■ 压力模型: SimUser per second
测试指标关注	<ul style="list-style-type: none">■ TCP Connection Per Second■ TCP Open Connections■ Network Throughput■ Total Failure Transactions

下表列出了实测结果。

指标	结果
TCP Connection Per Second	400,000
TCP Open Connections	16,000,000
Network Throughput (Gbps)	100
Total Failure Transactions	0

测试指标维持在上述叠加结果状态下，运行超过 30 分钟，系统表现稳定，如下图所示。

H3C SecPath M9000 测试报告



虚拟防火墙功能验证测试

虚拟防火墙重启功能

测试描述

ID	T_FUNC_VFW_RESTART
描述	通过仪表双臂部署模拟客户端和服务器并保持正常工作下的常规流量。两个虚拟防火墙实例同时处于工作状态。此时重启某个虚拟防火墙实例，确认系统业务不会受到此虚拟防火墙实例重启的影响。

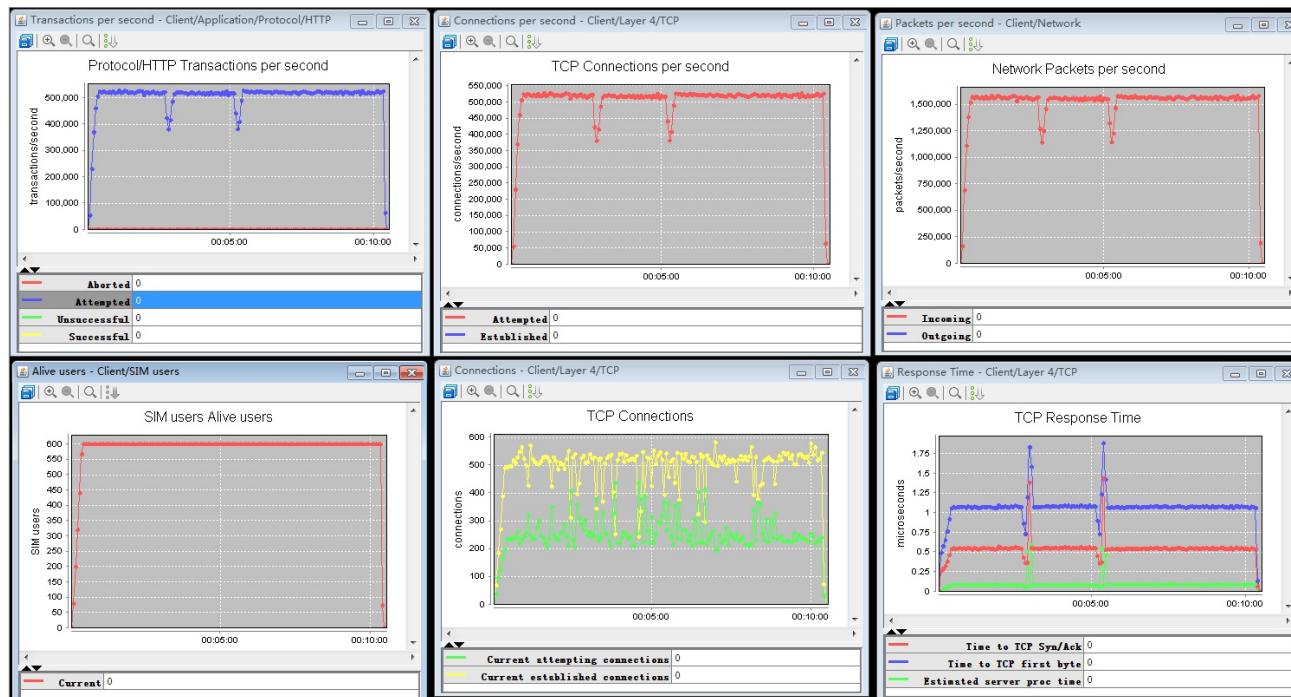
测试执行参数

测试执行参数	<ul style="list-style-type: none">■ IP 版本: IPv4■ 测试协议: HTTP■ 测试使用端口: 2 x 10G■ 压力模型: SimUser, 保持稳定的 CPS 输出
--------	--

H3C SecPath M9000 测试报告

测试指标关注	<ul style="list-style-type: none">■ TCP Connections Per Second■ Total Failure Transactions■ 系统状态变化恢复时间
--------	--

下图实测得到两个虚拟防火墙实例先后重启，对系统性能指标的影响。



结果表明：由上图可以看出，虚拟防火墙实例重启后会有非常短暂的系统响应降低，大约在10秒左右就可以恢复正常工作状态。重启虚拟防火墙实例没有对系统产生冲击和影响，系统运行状态良好。

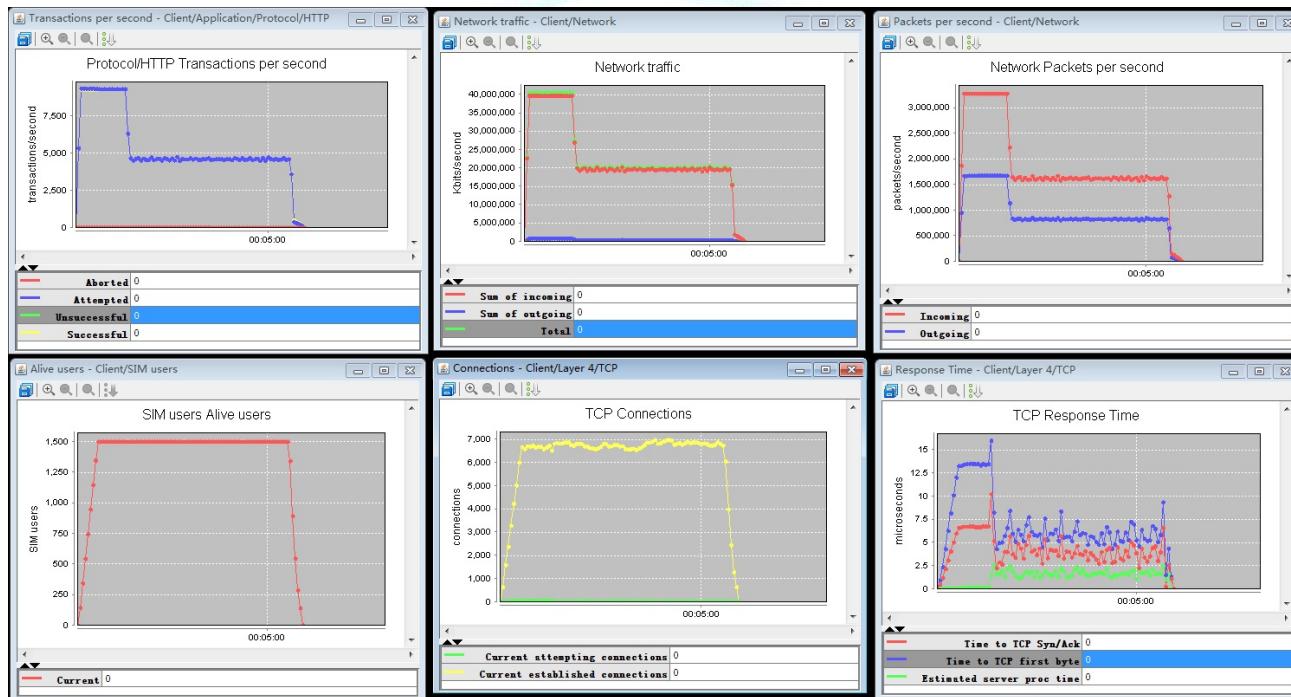
虚拟防火墙动态资源分配功能

测试描述	
ID	T_FUNC_VFW_DYNALLOC
描述	通过仪表双臂部署模拟客户端和服务器并保持正常工作下的常规流量。此时调整虚拟防火墙的资源设置，分别限制总吞吐、或 TCP 新建速率，系统应按照虚拟防火墙限定的资源设置运行。

H3C SecPath M9000 测试报告

测试执行参数	
测试执行参数	<ul style="list-style-type: none">■ IP 版本: IPv4■ 测试协议: HTTP■ 测试使用端口: 8 x 10G■ 压力模型: SimUser
测试指标关注	<ul style="list-style-type: none">■ TCP Connections Per Second■ Total Network Traffic (Throughput)

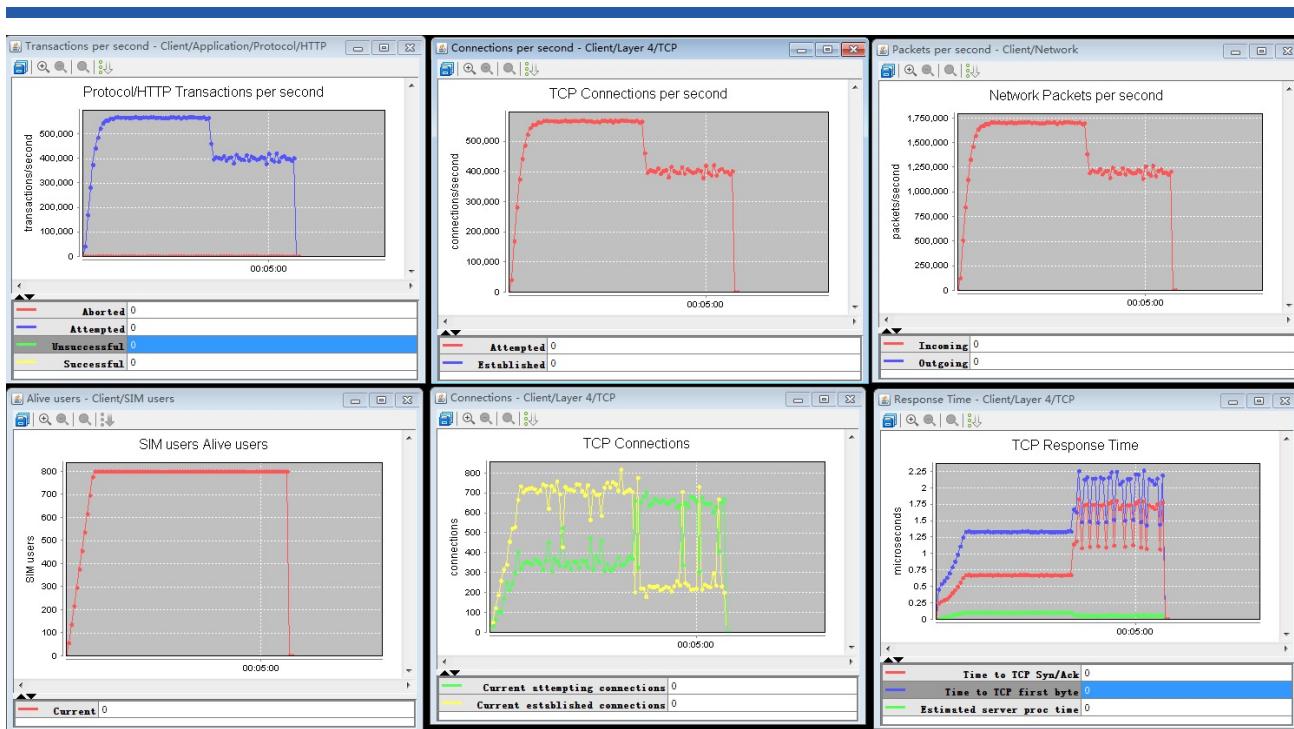
下图实测得到虚墙限制带宽上限由 40G 动态调整为 20G 后的行为曲线。



结果表明：带宽限定后，吞吐量严格按照调整后的限定运行。

下图实测得到虚墙限制 CPS 由 550,000 动态调整为 400,000 后的行为曲线。

H3C SecPath M9000 测试报告



结果表明：限定 CPS 上限后，系统运行基本保持在限定的 CPS 范围内，各项业务指标相应调整，运行正常。

网络特征攻防测试

典型攻击样本扫描检测

测试描述

ID	T_SEC_ATK_SCAN
描述	通过仪表双臂部署模拟客户端和服务器，选取 Spirent Test Cloud 中 2011-2016 年中典型攻击样本（约 250 个），利用 Spirent CyberFlood 的 CyberSecurity Assessment 测试方法进行攻击样本全扫描，得到系统对攻击样本的检出率。

测试执行参数

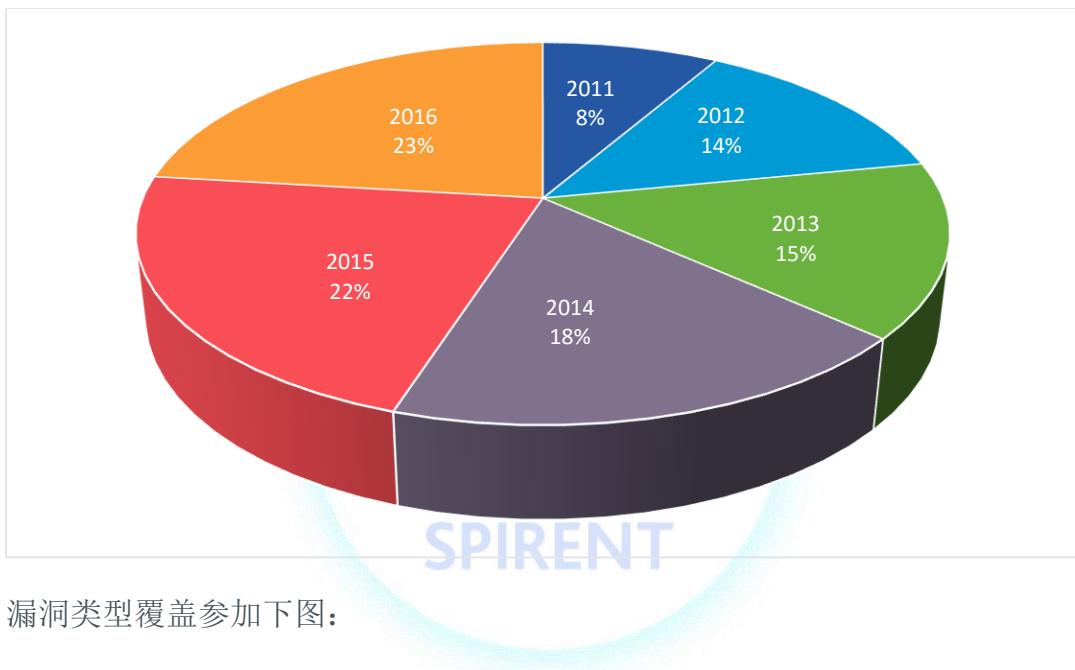
测试执行参数	<ul style="list-style-type: none">■ 测试方法模板： CyberSecurity Assessment■ 测试使用端口： 2 x 10G
--------	--

H3C SecPath M9000 测试报告

测试指标关注	■ 攻击检出率
--------	---------

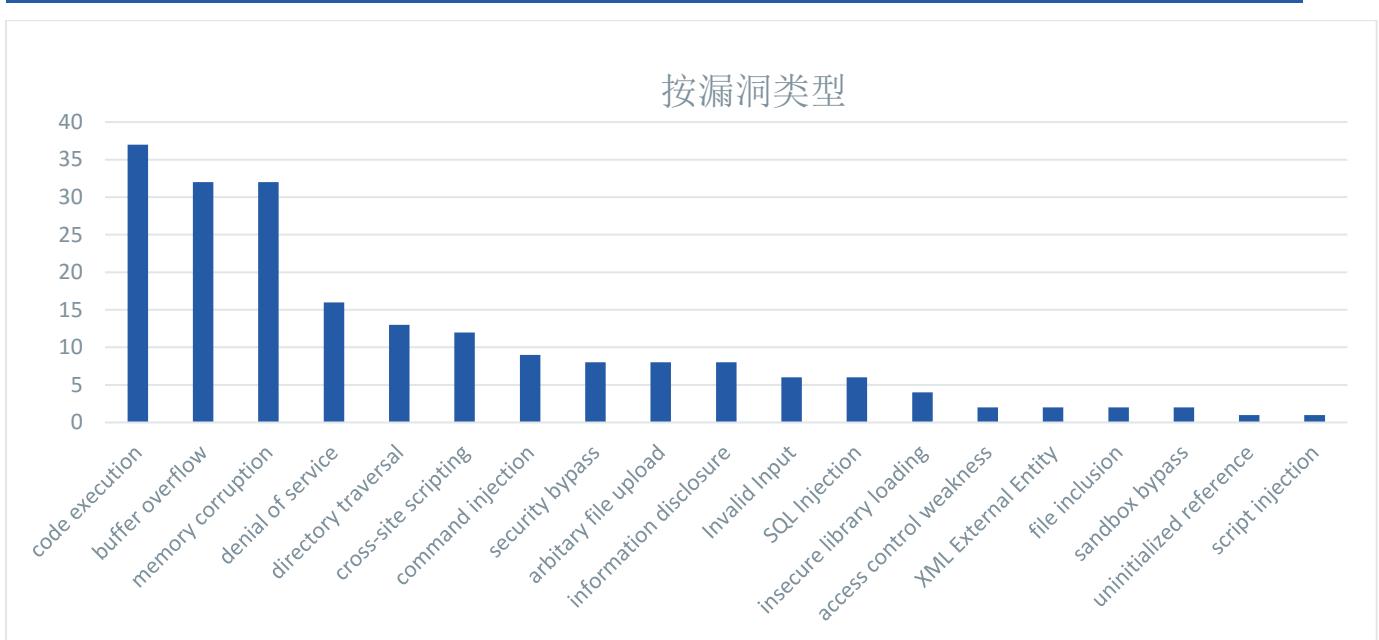
攻击样本的选择：

- ✓ CRITICAL/HIGH 高危漏洞样本占比超过 85%
- ✓ 服务器端软件漏洞和客户端软件漏洞占比分别为 53% 和 47%
- ✓ 各年度漏洞样本比例参加下图：



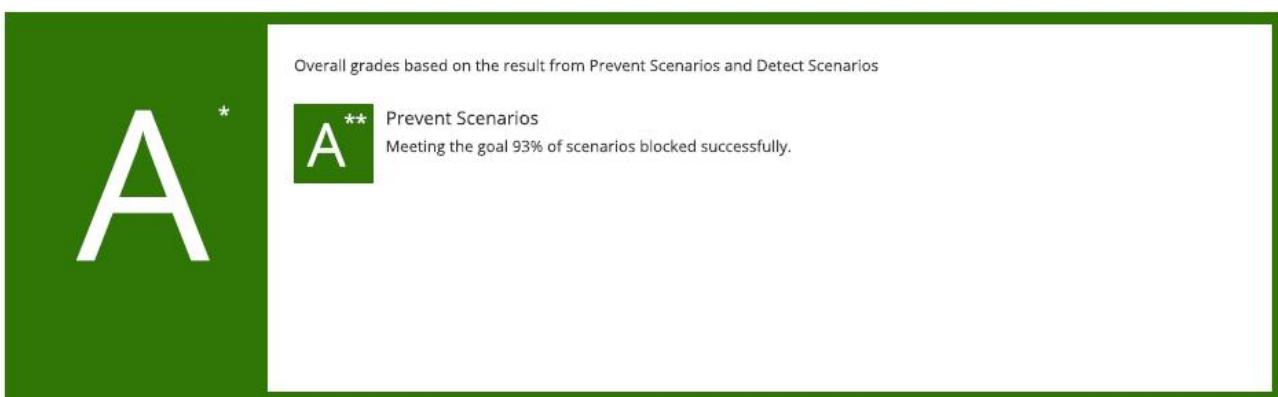
- ✓ 漏洞类型覆盖参加下图：

H3C SecPath M9000 测试报告



下面是攻击检出的评定结果。

|cyberflood TEST REPORT
CyberSecurity Assessment



H3C SecPath M9000 测试报告

防火墙 HA 可靠性测试

节点模块故障模拟下业务状态监测

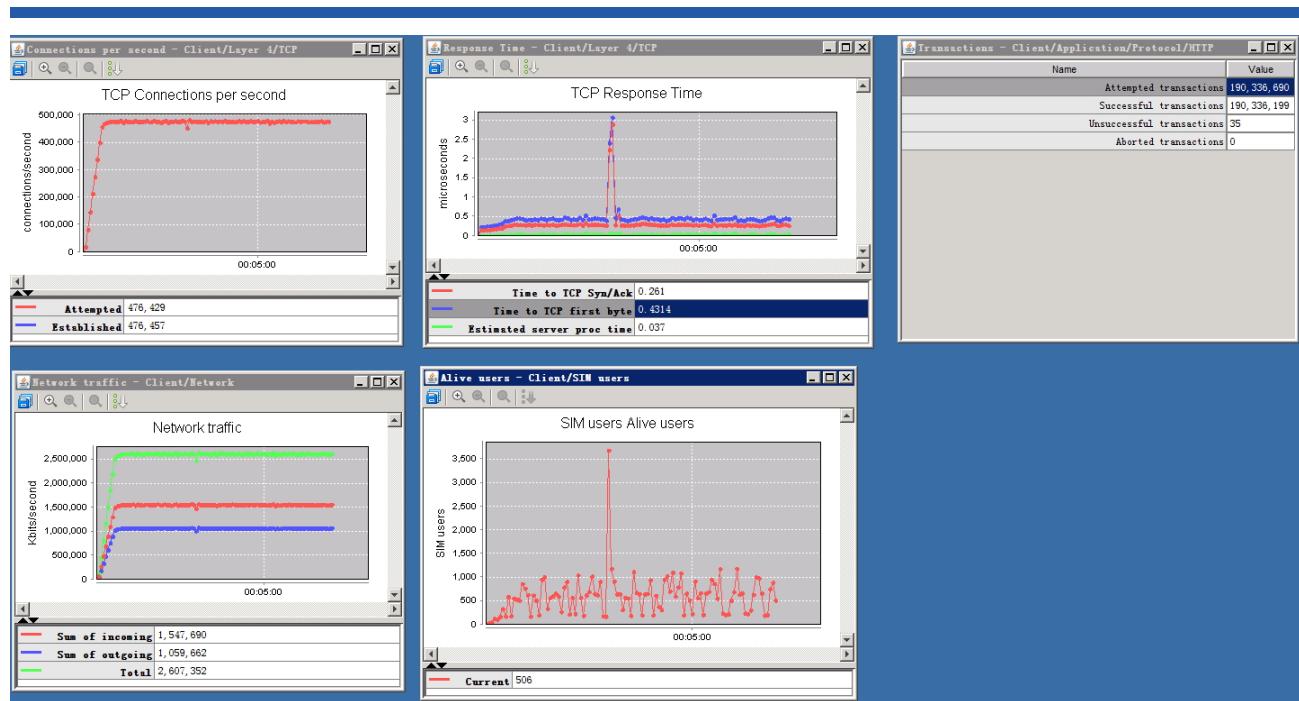
测试描述	
ID	T_RELFAULT_CHK
描述	
描述	通过仪表双臂部署模拟客户端和服务器，运行常规性能测试案例，在此过程中模拟设备各节点故障（主控故障，网板故障，主用链路故障，主用业务板故障），并在故障之后检查系统运行情况以验证单台 M9014 的冗余可靠性设计。
测试执行参数	
测试执行参数	<ul style="list-style-type: none">■ 背景测试流量：HTTP 应用带宽流量，约 2.6Gbps, CPS 476,000■ 测试使用端口：2 x 10G
测试指标关注	<ul style="list-style-type: none">■ 故障发生后的业务恢复时间■ 故障发生后到业务恢复之间的 Transaction 失败数量

实测结果表明：系统运行均可在各种故障状况下迅速恢复，只有微量的 transaction 失败影响。参见具体的各种故障实测效果如下。

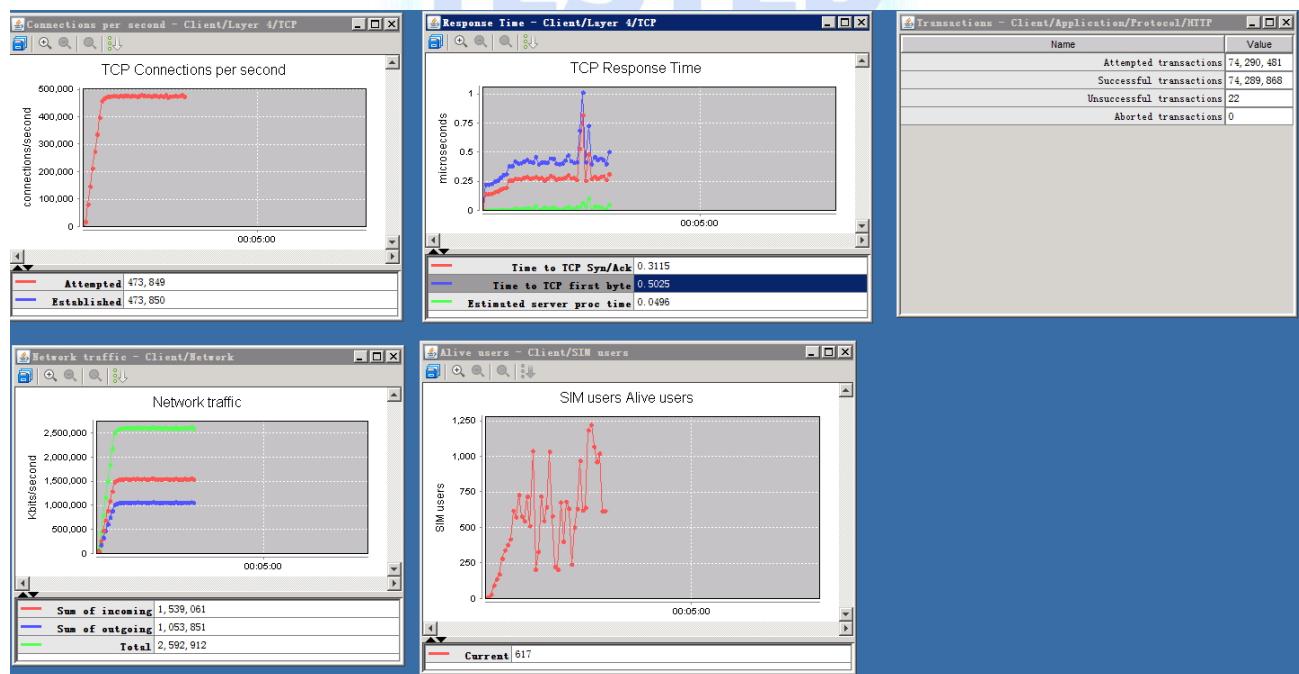
模拟主控板故障

手动拔出主用主控板的实测效果

H3C SecPath M9000 测试报告



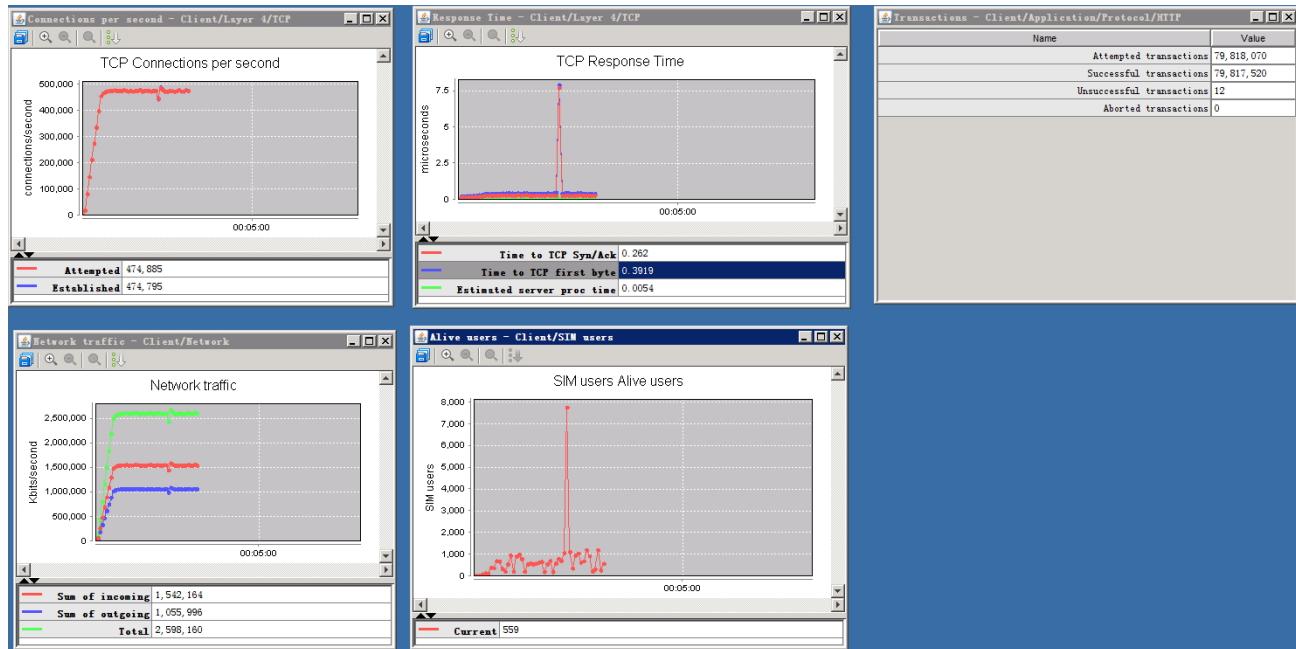
CLI 命令重启主用主控板的实测效果



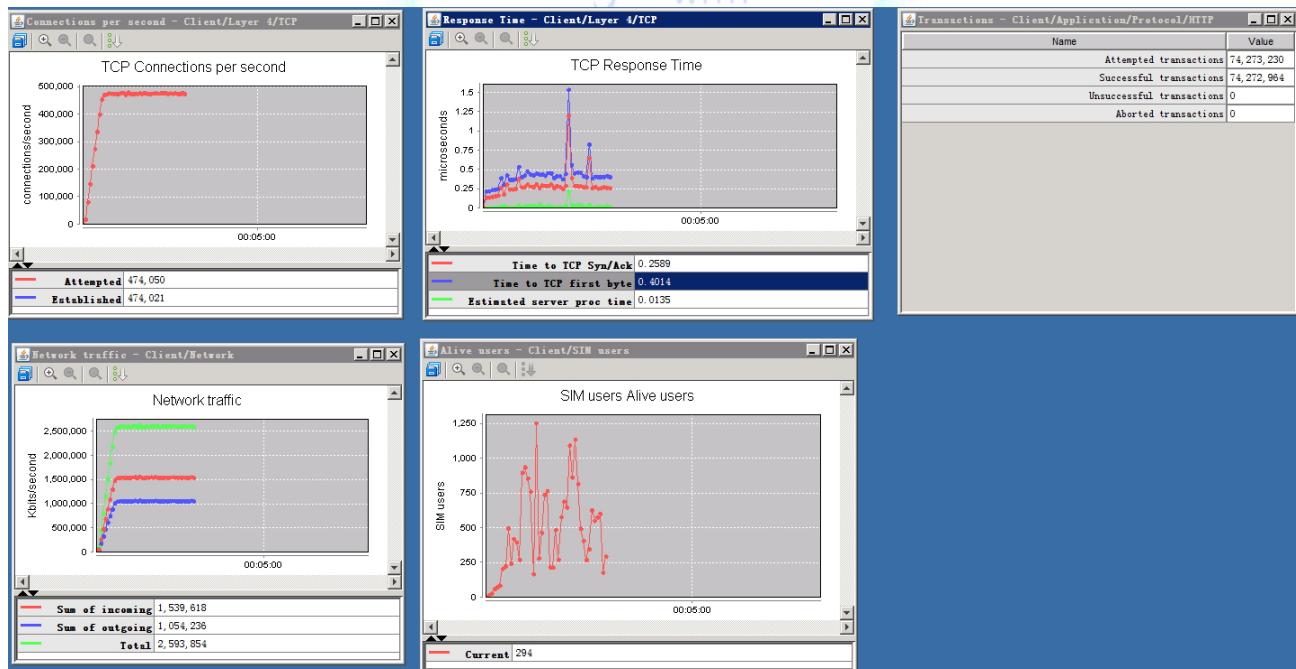
模拟网板故障

H3C SecPath M9000 测试报告

手动拔出网板的实测效果



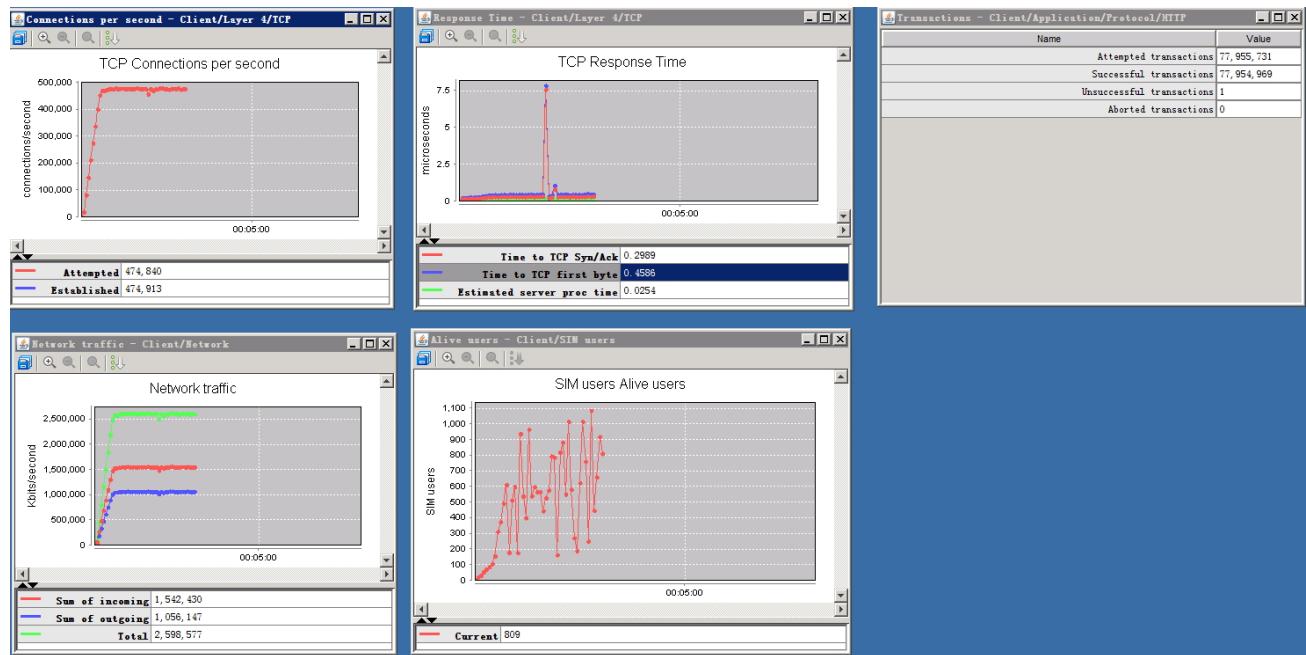
CLI 命令重启网板的实测效果



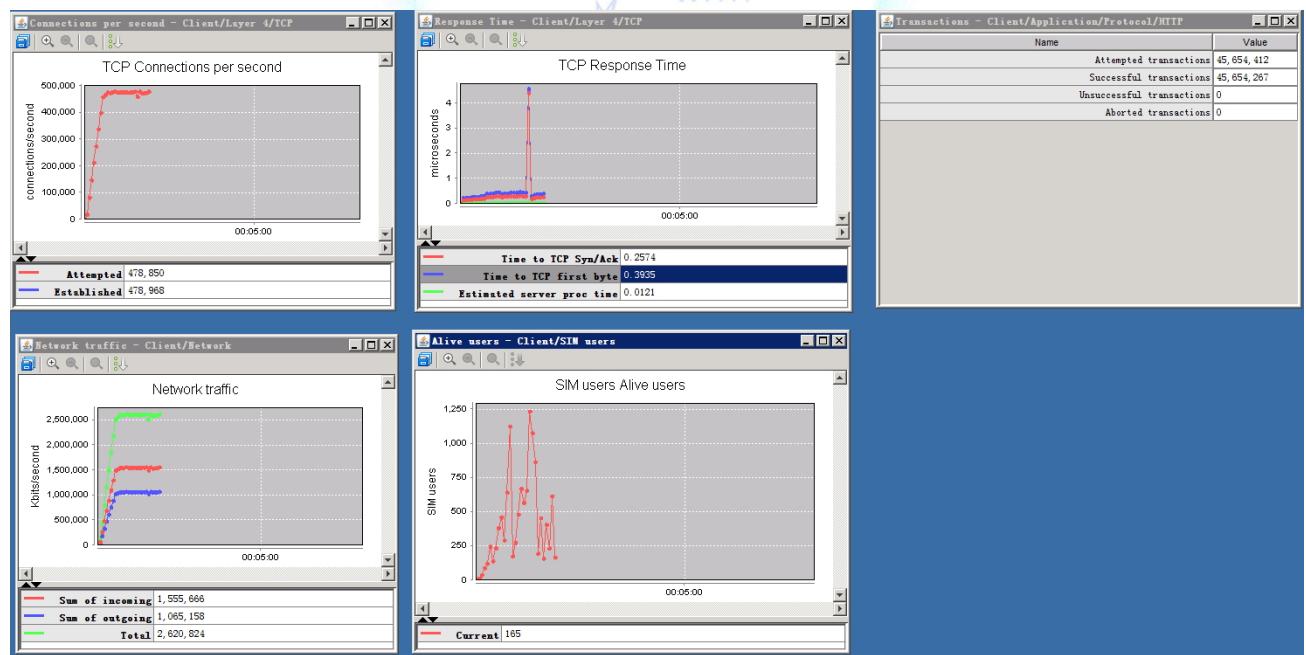
模拟主用链路故障

H3C SecPath M9000 测试报告

手动拔出主用链路光纤的实测效果



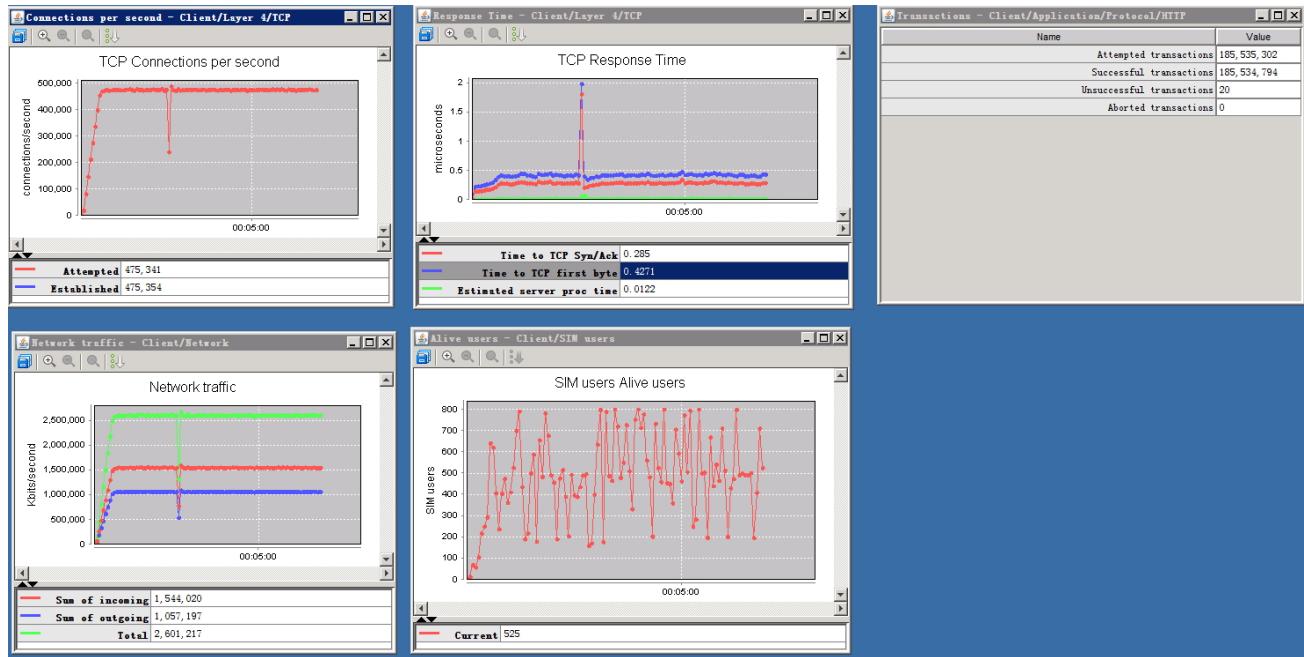
CLI 命令 shutdown 主用链路接口的实测效果



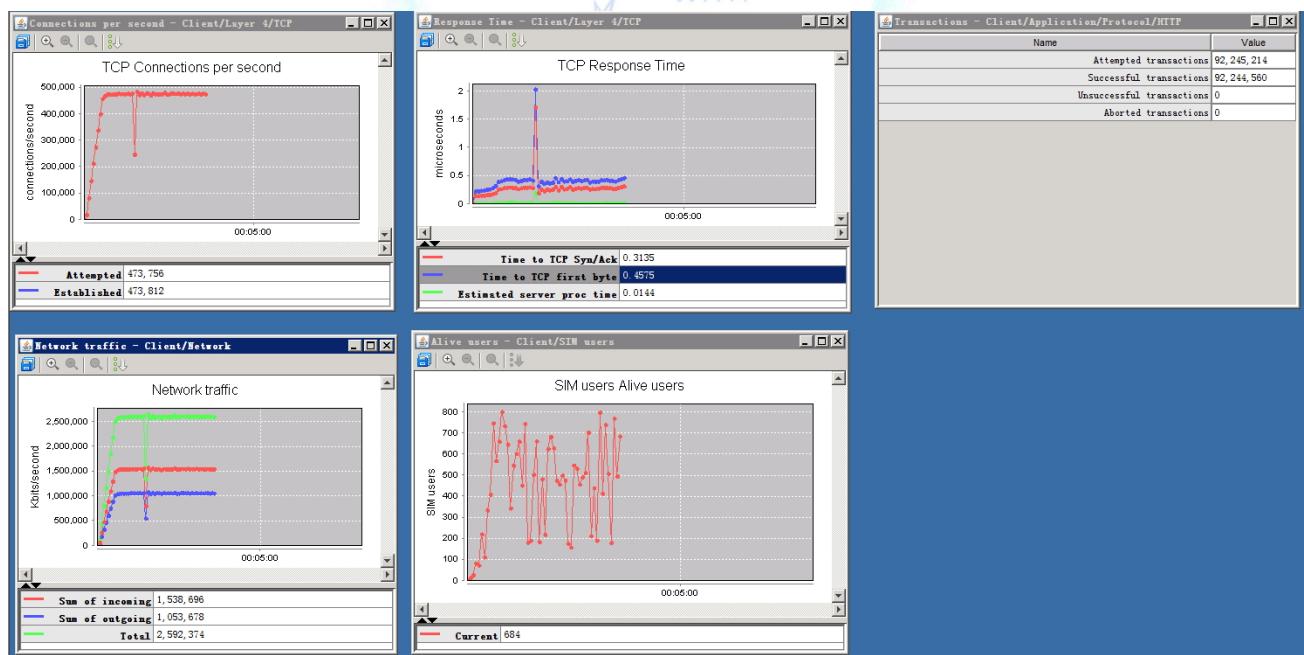
模拟业务板故障

H3C SecPath M9000 测试报告

手动拔出业务板卡的实测效果



CLI 命令重启主用业务板卡的实测效果



H3C SecPath M9000 测试报告

HA 双机故障模拟下业务状态监测

测试描述

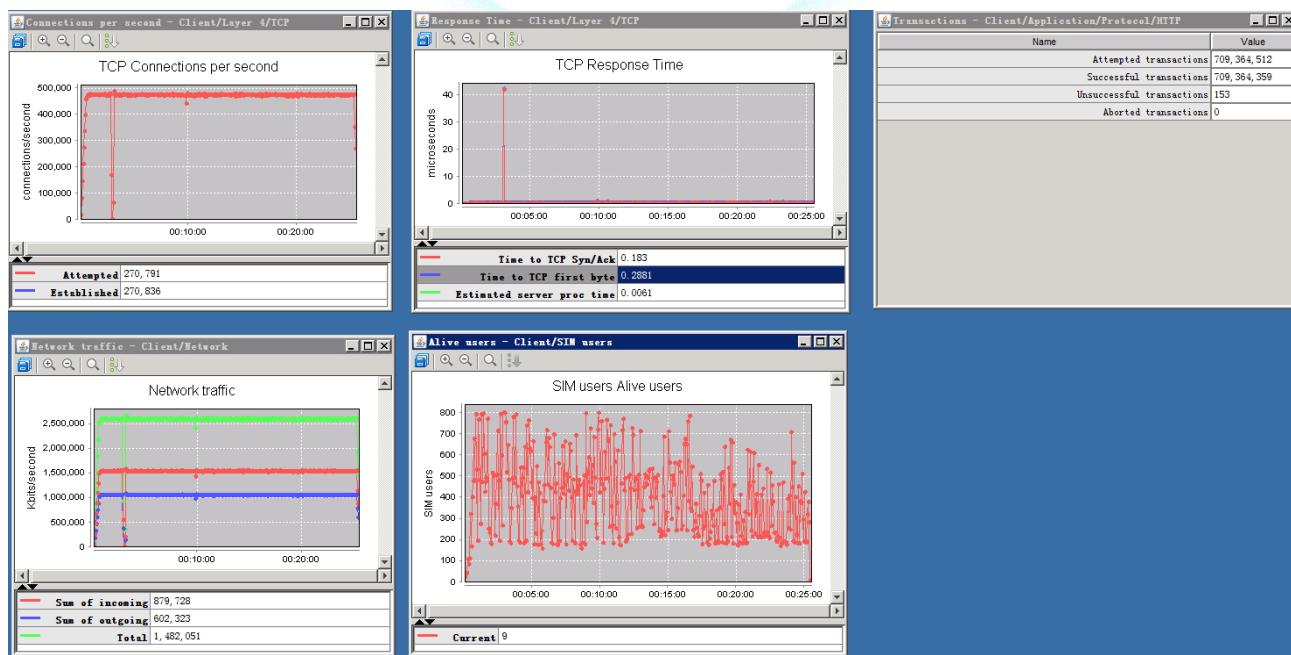
ID	T_RELFAULTCHK
描述	通过仪表双臂部署模拟客户端和服务器，运行常规性能测试案例，设备双机主备方式部署。在此过程中模拟设备主框节点的完全故障，并在故障之后检查系统运行情况以验证 M9014 的双机可靠性设计。

测试执行参数

测试执行参数	<ul style="list-style-type: none">■ 背景测试流量：HTTP 应用带宽流量■ 测试使用端口：2 x 10G
测试指标关注	<ul style="list-style-type: none">■ 故障发生后的业务恢复时间■ 故障发生后到业务恢复之间的 Transaction 失败数量

实测结果表明：系统运行可在主框故障状况下迅速恢复，只有微量的 transaction 失败影响。参见具体的故障实测效果如下。

手动主用主框掉电，并重新加电后恢复正常的效果



H3C SecPath M9000 测试报告

CLI 命令重新启动主用主框的实测效果

