文章编号:1671-4598(2025)07-0038-08 DOI:10.16526/j.cnki.11-4762/tp.2025.07.005 中图分类号:TP391.7 文献标识码:A

网络安全专用产品性能分类及测试方法研究

李 旋[1,2],陈 妍[1,2]
(1.公安部第三研究所 检测认证中心,上海 200031;
2.上海网络与信息安全测评工程技术研究中心,上海 200031)

摘要:为研究网络安全专用产品的性能指标,解决性能测试问题,对与不同网络安全专用产品配套使用的国家推荐标准进行了研究和分析,对标准中的性能要求进行了分类,将性能要求分为吞吐量延时、攻击检出、事件还原以及新建并发等大类,分类结果基本覆盖所有网络安全专用产品的性能要求;根据不同的性能分类设计了与其对应的基于虚拟化技术的改进的软件测试环境和方法,使用设计的软件测试方法对不同类型的网络安全专用产品进行了性能测试,同时与硬件仪表的测试结果进行了对比,设计的软件测试方法能够对性能指标进行有效的测试,得出可靠的测试结果。

关键词:网络安全专用产品;性能分类;性能测试;改进的软件测试;虚拟化

Research on Performance Classification and Testing Methods of Specialized Cybersecurity Products

LI Xuan[1,2], CHEN Yan[1,2]
(1. Testing and Certification Center, The Third Research Institute of Ministry of Public Security, Shanghai 200031, China;
2. Shanghai Engineering Research Center of Cyber and Information Security Evaluation, Shanghai 200031, China)

Abstract: In order to study the performance indicators of specialized cybersecurity products and solve the problem of performance testing, this paper studies and analyzes national recommended standards corresponding to different specialized cybersecurity products, and classifies performance requirements in the standards are classified into several major categories, including throughput latency, attack detection, event restoration, and concurrent creation, which basically covers the performance requirements of all specialized cybersecurity products. According to different performance classifications, the improved software testing environments and methods based on virtualization technology are designed, which tests the performance of different types of specialized cybersecurity products. Compared with testing results of instruments, the designed software testing method can effectively achieve the performance indicators of products and obtain reliable test results.

Keywords: specialized cybersecurity products; performance classification; performance testing; improved software testing; virtualization

0 引言

2023年4月国家相关部委联合发布了《关于调整网络安全专用产品安全管理有关事项的公告》,公告要求列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应当按照相关国家标准的强制性要求进行安全检测或认证,通过后方可销售或提供。2023年7月,国家更新了《网络关键设备和网络安全专用产品目录》(以下简称“网专目录”),网络关键设备和网络安全专用产品的类型得到了明确。以上两项公告的发布,对我国网络安全专用产品(以下简称“网专产品”)的检测和认证奠定了制度基础,网专产品的种类、覆盖范围得到了清晰的界定,解决了网络安全相关产品重复检测、认证以及产品归类不清的问题[1-2]。

美国和欧洲都有对网络安全产品的各自分类和管理规定,但分类规则与国内不同,且未形成统一的产品目

收稿日期:2025-02-06; **修回日期**:2025-03-17。
基金项目:国家标准项目(20230250-T-469)。
作者简介:李 旋(1987-),男,硕士,副研究员。
引用格式:李 旋,陈 妍.网络安全专用产品性能分类及测试方法研究[J].计算机测量与控制,2025,33(7):38-45.

录，而是通过一系列法规、标准、指南和认证体系来规范、管理和对相关的产品进行测评。我国的网专产品类型已形成体系且涵盖网络空间安全各个门类的相关产品。在进行网专产品检测、认证时按照国家强制标准 GB 42250-2022《信息安全技术 网络安全专用产品安全技术要求》进行，该标准作为基线标准提出了网专产品应具备的通用基本功能。此外，还需参考与特定网专产品配套的推荐标准，推荐标准中提出了该类产品特有的功能和性能要求。与网专产品配套的推荐标准主要为国家标准，在没有国家标准或者国家标准无法（不适合）进行产品测试时也使用原销售许可证制度下的公安行业标准。

目前由于相关的推荐性标准中对于网专产品的性能测试未给出明确和具体的测试手段、方法以及过程，因此性能测试方法是亟需研究、解决和统一的问题。本文将网专产品的性能进行了分类，在分类的基础上设计了不同的软件测试方法，明确和规范了测试方法，为产品的检测、认证提供了有力参考。

1　标准及产品性能分类

1.1　标准分类

网专目录中共包括 34 类产品，从采标类型来看，其中从第 1 类到第 19 类产品均具有与之配套的国家推荐标准。在国家推荐标准无法指导具体产品的测试时，也参考规范该类产品的公安行业标准，如安全数据库系统，在测试时通常使用 GA/T 1574-2019《信息安全技术 数据库安全加固产品安全技术要求》，如表 1 所示。此外，网专目录中从第 20 类网络型流量控制产品到第 34 类电子文档安全管理产品目前还没有与之配套的国家推荐标准，当前产品的检测工作仍参考与各个产品配套使用的公安行业标准，与这些产品类型配套的国家推荐标准在 2024 年 2 月通过了国家网络安全标准委员会立项或处于正在编制推进的过程中[3]。

表 1　网络安全专用产品配套的推荐标准

产品类别	参考标准
数据备份与恢复产品	GB/T 29765-2021 信息安全技术 数据备份与恢复产品技术要求与测试评价方法
防火墙	GB/T 20281-2020 信息安全技术 防火墙安全技术要求和测试评价方法
入侵检测系统(IDS)	GB/T 20275-2021 信息安全技术 网络入侵检测系统技术要求和测试评价方法
入侵防御系统(IPS)	GB/T 28451-2023 信息安全技术 网络入侵防御产品技术规范
网络和终端隔离产品	GB/T 20279-2024 网络安全技术 网络和终端隔离产品技术规范
反垃圾邮件产品	GB/T 30282-2023 信息安全技术 反垃圾邮件产品技术规范
网络安全审计产品	GB/T 20945-2023 信息安全技术 网络安全审计产品技术规范
网络脆弱性扫描产品	GB/T 20278-2022 信息安全技术 网络脆弱性扫描产品安全技术要求和测试评价方法
安全数据库系统	GB/T 20273-2019 信息安全技术 数据库管理系统安全技术要求 GA/T 1574-2019 信息安全技术 数据库安全加固产品安全技术要求
网站数据恢复产品	GB/T 29766-2021 信息安全技术 网站数据恢复产品技术要求与测试评价方法
虚拟专用网产品	GB/T 36968-2018 信息安全技术 IPSec VPN 技术规范 GA/T 686-2018 信息安全技术 虚拟专用网产品安全技术要求
防病毒网关	GB/T 35277-2017 信息安全技术 防病毒网关安全技术要求和测试评价方法
统一威胁管理产品(UTM)	GB/T 31499-2015 信息安全技术 统一威胁管理产品技术要求和测试评价方法
病毒防治产品	GB/T 37090-2018 信息安全技术 病毒防治产品 安全技术要求和测试评价方法
安全操作系统	GB/T 20272-2019 信息安全技术 操作系统安全技术要求
安全网络存储产品	GB/T 37939-2019 信息安全技术 网络存储安全技术要求
公钥基础设施	GB / T 21053-2023 信息安全技术 公钥基础设施 PKI 系统安全技术要求 GB / T 20520-2006 信息安全技术 公钥基础设施时间戳规范 GA 216.1-1999 计算机信息系统安全产品部件 第 1 部分:安全功能检测 4.4 密钥管理类产品
网络安全态势感知产品	GB/T 42453-2023 信息安全技术 网络安全态势感知通用技术要求
信息系统安全管理平台	GB/T 34990-2017 信息安全技术 信息系统安全管理平台技术要求和测试评价方法

1.2　性能要求及分类

性能指标是网专产品的重要技术指标，决定着产品的可用性，因此性能测试结果衡量了一个产品在一定负载下的功能强度。强制性国家标准 GB 42250-2022 中没有对网专产品的性能提出要求，因此在对网专产品的性能进行测试时主要根据与之配套的推荐标准中的性能要求进行。表 1 中大部分标准都对产品提出了性能要求，但是根据产品具体用途、形态和部署方式的不同，也有部分产品类型（如网络安全态势感知产品）未对自身的性能提出具体指标要求，仅在测试过程中记录测试时的软硬件配置、背景环境、条件等指标，为产品的性能提供参考。

推荐性标准中的性能要求条款对产品性能提出了具体要求，根据标准分类和要求，主要可分为吞吐量和延时类性能，如目录中的防火墙、网络和终端隔离产品、统一威胁管理产品（UTM）和虚拟专用网产品等类型

均要求对吞吐量以及延时进行测试；攻击检出类性能，如目录中的入侵检测系统（IDS）、入侵防御系统（IPS）、反垃圾邮件产品等类型均要求对攻击检出率进行测试；事件还原类性能，如目录中网络安全审计产品要求对可审计事件进行还原，对事件的采集和记录速度提出了具体要求，因该大类产品中包括了 4 种产品类型，在网络安全领域功能重要，因此本文对该类产品的性能进行了分类划分；新建并发类性能，如目录中防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）、统一威胁管理产品（UTM）、虚拟专用网产品等类型均要求对新建连接速率和最大并发连接数测试。

以上 4 类性能分类基本覆盖目录中所有网专产品的性能要求，包括正在制定的相关产品标准。本文将对以上 4 类性能分类进行研究和测试方法设计。此外，关于备份、恢复速度，监控响应时间等指标因仅出现在单个产品类型中且该类产品使用场景较其他大类少，迫切程度相对较低，该部分的性能指标本文未单独对其进行分类研究[4-5]。

2 性能测试方法及结果分析

第 1 章对网专产品的性能要求进行了分类，本章以具体的产品为例对标准中的性能要求进行分析研究、设计测试方法，给出上一章 4 类性能要求的测试方法，测试方法包括改进的软件测试方法以及使用硬件仪表在测试该类型产品时的常用设备及配置方法，通过测试实验对软硬件测试方法的测试结果进行比较和分析。

2.1 吞吐量延时类

2.1.1 性能要求分析

对于吞吐量和延时的定义在 RFC2544 中有较为详细的说明。在测试产品传输层吞吐量和延时性能时，通常参考 RFC2544 中的方法，采用 UDP 协议进行测试。本节以网专目录中的网络和终端隔离产品为例，对测试方法进行说明。GB/T 20279-2024 是关于网络和终端隔离产品的国家推荐标准，该标准中包括 4 种产品，其中对网闸和网络单向导入产品（以下简称隔离产品）提出了性能要求，性能指标根据产品自身的速率，吞吐量分为不小于 100 Mb/s、1 Gb/s 和 8 Gb/s，延时分为不大于 10 ms 和 5 ms[6]。

2.1.2 传统测试方法

iPerf 软件是用于测量 IP 网络带宽的工具，可以使用其发送穿过被测产品的报文，进行统计，完成吞吐量的测试。在测试延时指标时，可使用网络协议分析工具，如 Wireshark，分别在隔离产品的内部网络和外部网络上进行报文抓取，统计报文的通过时间，但是因隔离产品其独特的内部结构，具有连接内外网的不同主机，因此对于延时的测试会受到不同主机时钟不同步的影响，为了避免因时钟不同步导致的测试错误，传统的测试方法使用交换机配置镜像口的方式，将发送至隔离设备内部网络的报文和隔离设备外部网络发送至交换机的报文同时镜像至镜像物理机，使用镜像物理机的时钟计算同一个数据包分别离开和到达交换机的时间差来进行延时测试，如图 1 所示。

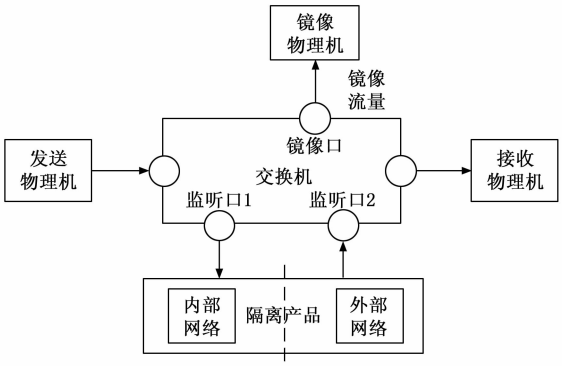

图 1 传统的吞吐量和延时测试方法原理图

虽然该测试方法巧妙的使用了交换机镜像的方式能够完成性能指标的测试，但是该方法需要使用多台计算机以及交换机构成测试系统，使用的设备多，测试环境不易移动维护[7-9]。

2.1.3 改进的软件测试方法

针对传统测试方法存在的问题，本节设计了一种使用一台测试物理机作为宿主机，通过虚拟化技术进行性能测试的改进的软件测试方法。该方法在测试物理机上部署 2 台虚拟机，虚拟化环境使用 VirtualBox 软件部署，VirtualBox 作为开源的跨平台虚拟化软件，具有虚拟机管理、资源分配等功能，能够保障测试系统的可靠性和稳定性。虚拟机上分别启动数据包发送和接收软件，并启用网络协议分析工具。相较于传统的由多台服务器构成的测试环境，该方法使用测试物理机提供了单一时间源，在不使用交换机的情况下，解决了时钟不同步的问题。使用在虚拟机上安装 iPerf 软件发送和接收数据包，统计和计算吞吐量，iPerf 作为专业的网络带宽测试软件，能够保障性能指标的可信度，使用 Wireshark（或 Tcpdump）在测试物理机的收、发端分别对穿过隔离设备的同一个数据包进行捕获，通过计算同一个数据包的发送和到达的时间差值可准确的进行延时指标的计算。该方法不仅降低了传统测试环境下需要使用多台服务器并通过交换机镜像导致的环境复杂，不易维护的问题，节约了测试设备，降低了成本，而且测试环境支持虚拟化方式的部署，在云原生不易串接其他硬件设备等的环境下，为云上部署的产品测试提供了参考，使用一台云环境中的宿主机或裸金属可完成测试环境的搭建。测试原理图如图 2 所示。

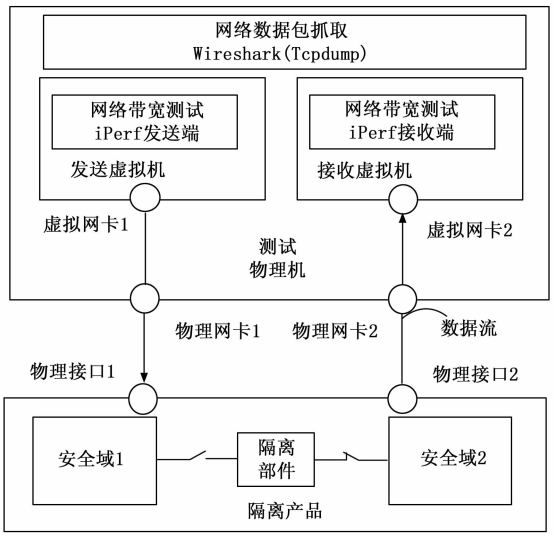

图 2　改进的吞吐量和延时软件测试方法原理图

2.1.4　实验验证与分析

在进行吞吐量和延时性能指标的测试时，通常会使用硬件仪表，硬件仪表可选用 ixia 测试仪的 IxNetwork 测试套件，选择 RFC 2544 测试模块，分别进行流配置（端口、IP 地址和传输方向等），协议选择（UDP 协议），流选项（字节大小在测试时选择 1 518 字节、设置起始延时等），测试参数（测试时间、测试的轮数等）等参数的配置。与软件测试原理类似，测试时将测试仪表与被测产品环路直连（串联部署）。硬件仪表的配置本文不做过多赘述。

为验证本文提出的改进的软件测试方法的可用性，测试时选取了 10 款网闸作为被测产品，产品在选择上，涵盖了国内主流网络安全厂商的主流产品，且覆盖产品主要的实现技术和不同的性能效率，以验证在不同技术实现及不同的性能效率下，改进的软件测试方法的有效性。分别使用改进的软件测试方法和硬件仪表的测试方法对选取的产品的性能进行测试，根据被测产品的接口速率，设置吞吐量测试指标的目标值，同时记录产品不丢包时最大吞吐量下的延时。测试采用 3 次结果取平均值的统计方式，两种方法下 10 款产品吞吐量的测试结果平均偏差率不大于 3%，延时的测试结果平均偏差率不大于 8%。其中 3 款产品的吞吐量和延时性能测试结果如表 2 所示。

表 2　网络隔离产品性能测试结果

性能指标		吞吐量/(MB/s)	延时/ms
产品 1	软件方法	1 844	1.19
	硬件仪表	1 895	1.28
产品 2	软件方法	2 807	0.27
	硬件仪表	2 721	0.23
产品 3	软件方法	1 970	1.88
	硬件仪表	1 973	1.86

2.2　攻击检出类

2.2.1　性能要求分析

攻击检出类的性能指标包括误拦截率、漏拦截率以及高流量背景下的入侵检测能力等。误拦截和漏拦截是针对攻击报文的发现能力，误拦截是错误的发现了或拦截了正常的流量，漏拦截是未发现或阻断带有攻击特性的流量。高流量背景下的入侵检测能力则是指在一定的网络带宽下完成攻击的检测能力。本节以网专目录中的网络入侵防御产品为例，在 GB/T 28451-2023 国家推荐标准中对于该类产品提出了性能要求，包括吞吐量、新建连接速率、并发连接数、误拦截率和漏拦截率。其中误拦截率和漏拦截率属于攻击检出类的性能测试指标，标准中对误拦截率要求应不超过 5%，漏拦截率应不超过 15%[10]。

2.2.2　传统测试方法

传统测试方法中，发送 PC 使用攻击发送软件发送带有攻击行为的网络报文并且经过运行分片变形程序的 PC 将流量发送至网络入侵防御产品，报文穿过入侵防御产品后到达目标服务器，通过统计已发送的攻击种类和数量以及被入侵防御产品识别和阻断的攻击种类和数量，计算产品的攻击检出能力，测试原理图如图 3 所示[11-12]。

该方法虽能完成性能测试工作，但是需使用较多的物理设备，物理环境复杂，不易于部署、移动和管理。

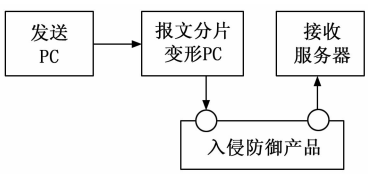

图 3　传统的攻击检出测试方法原理图

2.2.3　改进的软件测试方法

针对传统测试方法存在的问题，本节使用与测试吞吐量和延时性能指标类似的虚拟化技术对上一节由多台 PC 和服务器构成的传统测试环境进行了改进，改进后仅使用一台测试物理机作为测试设备，大大简化了测试环境。改进后的软件测试方法原理图如图 4 所示，以测试物理机作为宿主机，在宿主机上运行 VirtualBox 虚拟化软件、Blade 测试工具、搭建目标 Web 网站，在虚拟机中安装 Nikto、Fragrouter 和 Tcpreplay 等软件，构成整套测试环境，为虚拟机绑定工作在不同网络模式的虚拟网卡。

Blade 作为一个开源攻击框架，提供了基于网络层和应用层覆盖不同攻击阶段的诸多攻击类型。Nikto 是一款针对 Web 网站的开源攻击工具，除了常规的漏洞扫描、注入和拒绝服务攻击外，该工具还支持对攻击报

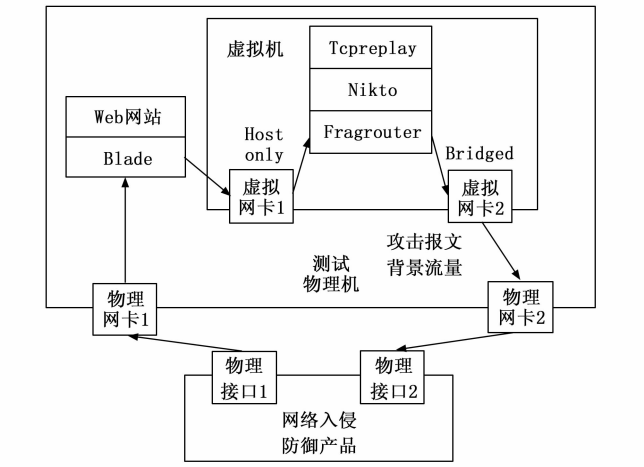

图 4 改进的攻击检出软件测试方法原理图

文进行变形，如使用反斜扛、随机字符串、URL 编码（非 UTF-8 方式）、自选路径（/./）等。Fragrouter 是一款网络入侵检测规避工具包，它能够对网络报文进行分片、重组，包括 IP 分片和 TCP 分段等，以达到逃避入侵检测（防御）产品发现的目的。将以上几种工具以一定的方式配合使用，可实现对入侵防御产品进行较为全面的测试。具体的，在测试时使用 Blade 由虚拟网卡 1（运行在 Host-Only 模式）经过虚拟网络 2（运行在 Bridge 模式绑定物理网卡 2）、物理网卡 2 向物理网卡 1 发送攻击报文，同时经过虚拟机中的 Fragrouter，将攻击报文分片重组后发出至被测产品。Nikto 则将针对 WEB 网站的变形攻击报文经虚拟网卡 2、物理网卡 2 发送到物理网卡 1，对测试物理机上的 Web 网站进行攻击，供被测产品进行攻击检测。Tcpreplay 是一套开源的软件工具集，主要用于网络流量重放和性能测试，使用 Tcpreplay 软件重放在真实网络环境中捕获的网络数据包，以及按照需要的带宽发出，模拟不含攻击特征的正常请求作为背景流量。此外，在本方法中还可以通过关闭 Fragrouter，进行未变形的原始攻击的测试。通过将实际发出的攻击数据包类型和数量与被测产品检出的结果进行比较，完成误拦截率和漏拦截率的性能检测[13-14]。

2.2.4 实验验证与分析

使用硬件仪表测试攻击检出时，可以选用 ixia Breakingpoint 仪表的 Security 功能模块，该模块能够提供标准化的攻击，包括代码变形、数据分片等，还能够将攻击数据打包为模板，便于重复使用。测试时将被测产品与测试仪表环路直连，选择攻击报文，调整攻击参数，如攻击时间、攻击轮数等，进行攻击测试，在仪表报告中可查看攻击被阻断的数量，得出测试结果。

选取 10 款网络安全入侵防御产品，涵盖不同厂商以及不同的攻击识别检测实现技术，如基于特征库、基于异常和基于行为的攻击检测技术等，以验证在不同技术实现原理下，改进的软件测试方法的有效性。分别使用改进的软件测试方法和硬件仪表的测试方法进行性能测试，测试在接口带宽 80％的背景流量下选取 183 种不同类型的攻击作为混合攻击，混合攻击中包括漏洞攻击、溢出攻击和 SQL 注入等，并对攻击方法进行躲避攻击设计，包括 HTTP 代码变形、IP 分片、TCP 分片等，测试 3 次取平均值，两种方法下 10 款产品误拦截率的测试结果平均偏差值不大于 0.01％，漏拦截率的测试结果平均偏差率不大于 3％。其中 3 款产品的测试结果如表 3 所示。

表 3 网络入侵防御产品性能测试结果

性能指标	误拦截率	漏拦截率/％	
产品 1	软件方法	0.00	12.97
	硬件仪表	0.00	13.11
产品 2	软件方法	0.02	44.24
	硬件仪表	0.03	43.17
产品 3	软件方法	0.01	34.97
	硬件仪表	0.01	33.88

2.3 事件还原类

2.3.1 性能要求分析

事件还原类性能主要指网专目录中的网络安全审计产品，在 GB/T 20945-2023 国家推荐标准中对于该类产品中的网络审计产品、数据库审计产品提出的性能要求包括数据采集速度和事件记录速度。数据采集速度是指在一定速率的背景流量下产品不漏审的速率，标准要求为采集接口速率 30％和 50％的背景流量下不漏审；事件记录速度是指通过流量采集方式获取审计数据，每秒可以审计的最大条数，标准要求为每秒 5 000 条和 10 000条。不管是数据采集速度还是事件记录速度，首先产品需要对流量中的网络协议进行收集和还原，在还原的基础上展现其事件分析的能力，因此，该类性能要求体现了审计类产品的事件还原能力[15]。

2.3.2 传统测试方法

传统测试方法如图 5 所示，客户端、服务器和审计产品分别与交换机连接，客户端连接在交换机的监听口上，安全审计产品连接交换机的镜像口，将客户端访问不同服务器的审计流量和背景流量均镜像至审计产品上，测试审计产品的流量捕获和还原能力。

该测试方法同样存在前文中所述的传统测试方法的缺点，需要使用较多的物理设备，测试环境和过程复杂，不易于部署、移动和管理，且需要根据不同的测试项目开启不同类型的服务器。

2.3.3 改进的软件测试方法

针对传统测试方法存在的问题，本节设计了一种改进的软件测试方法。使用构造流量的方式构造被审计事

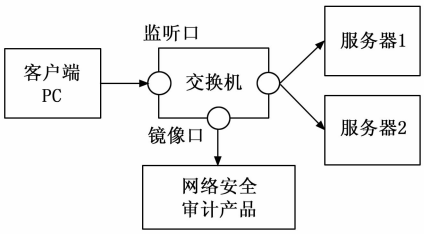

图 5　传统的事件还原测试方法原理图

件流量和背景流量的混合流量，通过数据报文回放软件供被测产品审计。根据性能指标间的计算关系，即在一定的事件发送速度（条/秒）下，通过调整数据报文的载荷，可计算出事件的流量大小，计算后可使用构造的数据报文通过 1 次回放测试，对 2 个性能指标同时进行测试，如在 5 000 条/秒的发送速率下，将每条可审计事件的载荷调整为 0.06 Mb，则可达到 300 Mbps 的流量带宽。相较于传统的测试方法，该方法不仅大大简化了由多台测试设备构成的测试环境复杂的问题，还提高了测试的效率。

测试原理图如图 6 所示，在测试物理机上安装 Tcpreplay 软件，对在实际网络环境中抓取的并根据测试需要进行按比例混合的数据报文进行回放，混合的数据针对被测产品的实际类型，需要包括标准中要求的 HTTP、SMTP、POP3、FTP 以及 SQL 等协议应用，使用测试物理机的物理网卡对已构造待回放的数据报文进行广播，审计产品的物理接口采集广播的数据报文，对采集到的数据报文进行分析和还原，通过对还原的事件数量进行统计，完成性能测试[16-18]。

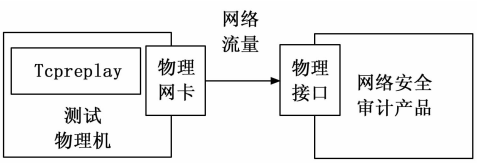

图 6　改进的事件还原软件测试方法原理图

2.3.4　实验验证与分析

使用硬件仪表测试事件还原能力时，可以选用 ixia Breakingpoint 测试仪的 Application Simulator 功能模块，该模块能够生成 2～7 层的真实网络流量，在该功能模块的 Parameters 配置界面中可以对应用类型、数据速率、新建并发和持续时间等参数进行配置，在测试时根据测试需求发送相应速率的数据报文，通过查阅测试仪发送的数据量以及被测产品审计到的数据量，记录测试结果。

选取 10 款网络安全审计产品，为涵盖不同审计类型的产品，其中网络审计产品 6 款，数据库审计产品 4 款，来自不同的网络安全厂商，分别使用改进的软件测试方法和硬件仪表的测试方法进行测试，测试产品的性能，测试 3 次取平均值。两种方法下 10 款产品数据采集速度的测试结果平均偏差率不大于 2%，事件记录速度的测试结果平均偏差率不大于 10%。其中 2 款网络审计产品和 1 款数据库审计产品（产品 3）的测试结果如表 4 所示。

表 4　网络安全审计产品性能测试结果

性能指标	数据采集速度	事件记录速度	
产品 1	软件方法	391.0 Mbps	6 890.3 条/秒
	硬件仪表	389.0 Mbps	6 942.9 条/秒
产品 2	软件方法	952.0 Mbps	13 960.1 条/秒
	硬件仪表	950.3 Mbps	15 425.4 条/秒
产品 3	软件方法	462.0 Mbps	35 960.4 条/秒
	硬件仪表	461.3 Mbps	35 485.9 条/秒

2.4　新建并发类

2.4.1　性能要求分析

新建并发类的性能指标即新建连接速率和并发连接数，包括传输层和应用层。具体以网专目录中的防火墙为例，在 GB/T 20281-2020 国家推荐标准中对于网络型防火墙、WEB 应用防火墙和数据库防火墙均提出了该类型的性能要求，包括 TCP 新建连接速率和并发连接数、HTTP 和 SQL 请求速率和并发连接数[19]。

2.4.2　软件测试方法

JMeter 软件是一款对功能行为进行负载测试并衡量被测系统性能的开源软件，该软件能够对不同类型的协议进行性能压力测试，包括传输层的 TCP 协议和应用层的 HTTP 协议等。JMeter 支持主从模式，即通过一个终端控制多个终端共同对被测产品进行数据包发送，基于此，本节使用虚拟化技术设计了一种软件测试方法，如图 7 所示。该方法使用一台测试物理机作为测试设备，在其上安装测试网站作为目标机，并启用一定数量的虚拟机或容器构成测试环境。

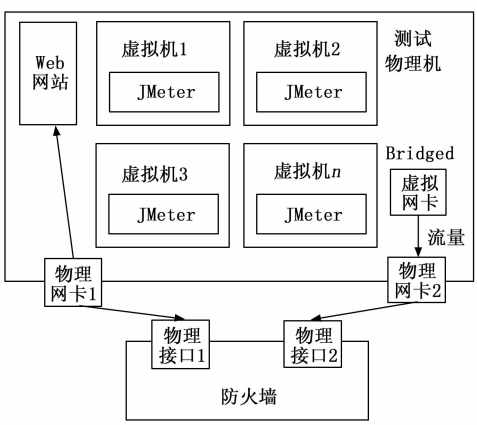

图 7　新建并发软件测试方法原理图

以 VirtualBox 软件搭建虚拟机的方式作为测试环境，在测试物理机上根据实际需要发出的连接数启用不同数量的虚拟机，虚拟机上安装 JMeter 软件并配置发送速率，通过测试物理机的物理网卡 2 向被测产品发送请求，被测产品将请求转发到测试物理机的物理网卡 1 上，并最终到达 Web 网站（HTTP 新建和并发测试）。新建和并发的测试可以使用相同的测试模板，在测试新建连接速率时，在设定值下持续发出新建连接请求并拆除已建立的连接，使发出的连接速率保持在一定值，查看产品的连接数是否能够保持在该设定值，而在测试并发连接数时则保持已建立的连接，查看产品是否能够到达并发连接数的设定值，对成功建立的请求数量进行统计，完成被测产品的性能测试[20]。

2.4.3 实验验证与分析

使用硬件进行新建和并发测试时，可以选用 ixia Breakingpoint 仪表的 SessionSender 和 Application Simulator 功能模块，SessionSender 模块能够生成 TCP 协议的网络请求，用于测试 TCP 新建连接速率和并发连接数，Application Simulator 功能模块在上一节已做介绍，可生成 HTTP、SQL 应用协议的网络连接请求，根据测试的性能指标调整硬件仪表的发包速度，可对产品的性能进行测试。

选取不同网络安全厂商以及不同性能接口速率的 10 款防火墙，分别使用软件测试方法和硬件仪表的测试方法对 TCP 新建连接率和并发连接数性能指标进行测试，测试 3 次取平均值，两种方法下 10 款产品新建的测试结果平均偏差率不大于 0.5%，并发的测试结果平均偏差率不大于 0.5%。其中 3 款产品的测试结果如表 5 所示。

表 5 防火墙 TCP 新建连接率和并发连接数测试结果

性能指标	新建连接率	并发连接数	
产品 1	软件方法	5 497 个/秒	21 940 个
	硬件仪表	5 500 个/秒	22 000 个
产品 2	软件方法	5 490 个/秒	21 977 个
	硬件仪表	5 500 个/秒	22 000 个
产品 3	软件方法	5 489 个/秒	21 969 个
	硬件仪表	5 500 个/秒	22 000 个

2.5 测试结果分析

从表 2～5 中具体的产品测试结果可以看出，针对不同类型的性能要求，与硬件仪表的测试方法相比，文中设计的各种软件测试方法均能够得出类似的测试结果，测试结果的偏差反映了产品的性能波动，偏差在可以接受的正常范围内。表 5 中针对防火墙，测试时在标准要求应达到指标的基础上增加了 10%的性能指标要求，以使测试过程中因被测产品的性能波动的情况下，测试结果仍能够满足标准中的要求，其他产品的测试结果则为测试环境下的实际值或产品的性能最优值。测试新建和并发指标时，硬件测试仪表因能够发出测试所配置固定的目标值，且产品能够正常建立连接，因此 3 款产品的测试结果均稳定在目标值上，而软件测试方法因使用的软件在发包时存在抖动以及爬坡时间，导致每次发包结果不是固定值，但是因设置了 10%的余量，通过防火墙建立的连接数量与软件实际发出的连接数量相比，仍能得出准确、可靠的测试结果。

从文中对不同类型的 10 款产品的测试结果进行统计分析可以得出，针对吞吐量和延时指标，吞吐量的偏差值不大于 30 Mb/s，延时偏差值不大于 0.4 ms；针对攻击检出指标，误拦截率的偏差值不大于 0.01%，漏拦截率的测试结果偏差值不大于 4.5%；针对数据采集速度的事件记录速度，数据采集速度的偏差值不大于 0.6%，事件记录速度的偏差值不大于 50 条/s；针对新建连接数和的并发连接数，新建连接数的偏差值不大于 25 个/s，并发连接数的偏差值不大于 1000 个。测试偏差均以绝对值的方式进行统计，且偏差值均未超过目标值的 3%，在合理的波动范围内，因此，在多次测量取平均值的测试方法下，不会因软硬件测试方法的不同导致对产品性能结果是否符合造成误判。

3 结束语

本文从网专产品在检测、认证时采用的国家推荐标准入手，对标准要求的性能指标进行了分析和分类，归纳出了 4 种性能要求大类，针对不同类型的性能要求大类设计了优化改进的软件测试方法，并以具体的网专产品为例对设计的方法进行了性能测试，得出了与使用硬件仪表测试的类似结果，且测试结果在误差范围内，能够测出产品可靠的性能值。与传统的测试方法相比，文中设计的测试方法因用到了虚拟化等技术，简化了测试环境，提高了测试的效率。同时，在硬件仪表不易获取或在产品开发自测阶段时，可参考使用本文给出的软件测试方法对网专产品进行性能测试。此外，本文还为产品上云后，不便使用硬件设备进行测试时提供了可供参考的性能测试解决方案。

参考文献：

[1] 国家互联网信息办公室. 关于调整网络安全专用产品安全管理有关事项的公告 [EB/OL]. (2023-04-17) [2025-01-10]. http://www.cac.gov.cn/2023-04/17/c_1683373663-312410.htm.

[2] 国家互联网信息办公室. 关于调整《网络关键设备和网络安全专用产品目录》的公告 [EB/OL]. (2023-07-03) [2025-01-11]. http://www.cac.gov.cn/2023-07/03/c_1690034742530280.htm.

[3] 全国网络安全标准化技术委员会. 关于 17 项网络安全国家标准项目立项的通知 [EB/OL]. (2024-02-19) [2025-01-11]. https://www.tc260.org.cn/front/postDetail.html? id=20240219162130.

[4] 孟珞珈，郭元兴，盛强强，等. 模块类网络安全产品的智能测试系统设计 [J]. 计算机测量与控制，2024，32 (1)：37－44.

[5] 罗　晋，骆　超，赵　祺，等. IPsec 产品自动化测试系统设计 [J]. 计算机测量与控制，2024，32 (11)：80－86.

[6] 全国信息安全标准化技术委员会. GB/T 20279-2015 信息安全技术网络和终端隔离产品安全技术要求 [S]. 北京：中国标准出版社，2024.

[7] 李　旋，顾建新，李　毅. 网络安全专用产品网闸性能测试方法设计 [J]. 计算机系统应用，2019，28 (1)：233－238.

[8] 崔津华，蔡志平，刘柯江. SGX 隔离技术研究综述 [J]. 华中科技大学学报 (自然科学版)，2024，52 (2)：1－15.

[9] 李　旋，吴其聪，沈　亮，等. 实现对网络隔离产品性能进行测试控制的系统及方法 [P]. 中国：ZL2018 1 1331953.0. 2024－05－17.

[10] GB/T 28451-2023 全国信息安全标准化技术委员会. 信息安全技术 网络入侵防御产品技术规范 [S]. 北京：中国标准出版社，2023：6－7，22－24.

[11] 蹇诗婕，卢志刚，杜　丹，等. 网络入侵检测技术综述 [J]. 信息安全学报，2020，5 (4)：96－122.

[12] LI X，GU J，LI Q. Testing methods research and design for NIPS anti-evasion attack [J]. ACSR-Advances in Computer Science Research，2015：16－19.

[13] 牛月坤，曹　慧，田晨雨，等. 基于机器学习的自动化渗透测试系统技术的研究 [J]. 计算机测量与控制，2022，30 (6)：17－22，31.

[14] 周　琰，马　强. 基于混合模式匹配算法的网络入侵检测 [J]. 计算机测量与控制，2022，30 (11)：65－70.

[15] GB/T 20945-2023 全国信息安全标准化技术委员会. 信息安全技术 网络安全审计产品技术规范 [S]. 北京：中国标准出版社，2023，10：27－28.

[16] SERGEJA SLAPNICAR，TINA VUKO，MARKO CULAR，et al. Effectiveness of cybersecurity audit [J/OL]. International Journal of Accounting Information Systems，2022：4－18. [2025-01-20]. https://doi.org/10.1016/j.accinf.2021.100548.

[17] 符永铨，赵　辉，王晓锋，等. 网络行为仿真综述 [J]. 软件学报，2022，33 (1)：274－296.

[18] 邹志博. 基于数据挖掘的自适应网络安全审计系统的研究与实现 [J]. 软件，2022，43 (10)：145－147.

[19] 全国信息安全标准化技术委员会. GB/T 20281-2020 信息安全技术 防火墙安全技术要求和评价方法 [S]. 北京：中国标准出版社，2020.

[20] DMITRIJ MELKOV，ARUNAS SALTIS，SARUNAS PAULIKAS. Performance testing of linux firewalls [J]. 2020 IEEE Open Conference of Electrical，Electronic and Information Sciences，2020：1－4.

(上接第 37 页)

[7] BYINGTON C S，WATSON M，EDWARDS D. A model-based approach to prognostics and health management for flight control actuators [C] // Aerospace Conference，2004，Proceedings. IEEE，2004 (6)：3551－562.

[8] HAN T，HUANG H S，YAO L G. Entity extraction for aero-engine fault knowledge graph [J]. Modular Machine Tool & Automatic Manufacturing Technique，2021 (10)：69－73.

[9] GUANG R Z，SHI Q L，YUAN J S，et al. LPV robust servo control of aircraft active side-sticks [J]. Aircraft Engineering and Aerospace Technology，2020，92 (4).

[10] FERGANI S，ALLIAS J F，BRIERE Y，et al. A novel structure design and control strategy for an aircraft active side stick. Mediterranean Conferenceon Control and Automation. MED. IEEE，2016：1114－1119.

[11] JAYARAMAN G，SZULYK Z. Active sidestick design using impedance control [C] // 2009 IEEE International Conference on Systems，Man and Cybernetics，Oct 11－14，2009. San Antonio，TX，USA：IEEE，c2009：4432－4437.

[12] 程　义. 精密行星减速器的回差分析与公差设计 [D]. 大连：大连理工大学，2021.

[13] 王　灿，杨　忠，陈　旭. 飞机 ASS 非线性系统的建模与控制 [J]. 应用科技，2023，50 (5)：157－162.

[14] 王婧茹，王　博，王宜芳. 新型飞控驾驶舱操纵机构故障状态建模与分析 [J]. 航空工程进展，2015，6 (3)：354－359.

[15] 王少萍，陶建峰，焦宗夏. 基于仿真模板的控制系统可靠性分析 [J]. 北京航空航天大学学报，2004 (9)：813－817.

[16] 张　蓉，王春洁. 基于 FMEA 和 FTA 的三自由度直角坐标机器人系统可靠性仿真分析 [J]. 机械科学与技术，2006 (6)：651－654.

[17] 李冰月，孙建红，刘海港. 基于 FMEA 的飞机空调系统故障诊断与仿真 [J]. 振动·测试与诊断，2017，37 (3)：588－595.

[18] 成振华. 基于神经网络的直流电机在线故障诊断研究 [D]. 广州：华南理工大学，2017.

[19] 孙子明. 基于参数优化 VMD 及卷积神经网络的电机轴承故障诊断研究 [D]. 扬州：扬州大学，2023.

[20] 柳　杨，王　凌，高雁凤. 工业机器人谐波减速器的传动误差超限故障诊断 [J]. 机床与液压，2021，49 (17)：185－190.