计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2019,28(1):233−238 [doi: 10.15888/j.cnki.csa.006725]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

网络安全专用产品网闸性能测试方法①

李　旋, 顾建新, 李　毅

(公安部第三研究所 检测中心, 上海 200031)
通讯作者: 李　旋, E-mail: lixuan@mctc.org.cn

摘　要: 为解决网络安全专用产品网闸的性能测试问题, 研究了针对网闸产品性能的测试方法, 设计了包括使用iPerf 软件和 IXIA 硬件的两种测试方式, 两种测试方式均能够适用于对网闸性能的测试. 同时, 还分析了国家标准中对网闸性能要求的测试方法, 并与网络安全专用产品的性能要求做了对比说明, 最后通过实验的方式, 测试了网络安全专用产品中网闸的吞吐量和系统延时性能指标, 给出了 14 款网闸产品的性能结果分布.

关键词: 网络安全专用产品; 网闸; 性能测试

引用格式: 李旋,顾建新,李毅.网络安全专用产品网闸性能测试方法.计算机系统应用,2019,28(1):233–238. http://www.c-s-a.org.cn/1003-3254/6725.html

Performance Test Method for Gap in Network Security Special Products

LI Xuan, GU Jian-Xin, LI Yi

(Testing Center, the Third Research Institute, Ministry of Public Security, Shanghai 200031, China)

Abstract: To solve the problem of performance testing for gap of network security special products, a test method for gap performance was studied. Two test methods including the use of iPerf software and IXIA hardware were designed. Both test methods can be applied to the test of gap performance. At the same time, a test method for the performance requirements of gap in the national standards was also analyzed, and a comparative analysis was made with the performance requirements of network security special products. Finally, the throughput and system delay performance for the gap of network security special products are tested through experiments. The distribution results of the 14 gap products are given.

Key words: network security special products; gap; performance test

国家互联网信息办公室联合信息化部、公安部、国家认证认可监督管理委员会等部门于 2017 年发布了一批网络关键设备和网络安全专用产品的目录, 目录内的设备和产品需按照国家标准的要求进行强制认证和检测, 进一步体现了国家对网络安全的重视. 网络安全产品—安全隔离与信息交换产品 (网闸) 出现在本次公布的目录之内, 且在目录中给出了网闸产品进入网络安全专用产品需要具备的条件. 条件中明确的对网闸性能进行了要求, 即吞吐量≥1 Gbps, 系统延时≤5 ms[1].

国标《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》中对于网络隔离产品也具有性能要求, 即交换速率大于 1000 Mbps, 硬件切换时间小于 5 ms. 本文针对网络安全专用产品以及国标中的性能要求分别设计了网闸产品的性能测试方法, 并通过实验进行分析[2,3].

1　网络隔离产品介绍

1.1　网络隔离产品分类

网络隔离产品主要分为网闸和协议隔离. 网闸在结构上以二主机加专用隔离部件的方式组成, 即由内

① 基金项目: 国家重点研发计划 (2016YFB0800903)
Foundation item: National Key Research and Development Program of China (2016YFB0800903)
收稿时间: 2018-05-16; 修改时间: 2018-06-08; 采用时间: 2018-08-15; csa 在线出版时间: 2018-12-26

部处理单元、外部处理单元和专用隔离部件组成, 内部处理单元通常连接内部安全域, 外部处理单元连接外部安全域, 专用隔离部件对两个安全域进行物理上的断开, 同时满足数据的交换. 网闸除了实现不同安全域之间的物理断开之外, 在软件功能上还具有身份认证、访问控制、协议剥离等功能, 从而保证不同网络之间数据交换的安全性.

协议隔离也起到不同安全域之间的安全数据交换, 但是在物理结构上只要求二主机, 并没有强制要求二主机之间具有专有隔离部件, 而是采用协议剥离和转换的方式保证安全. 即两个安全域之间进行数据交换时, 协议隔离产品剥离了 TCP/IP 协议, 转换为私有协议进行通信和数据传输. 因此协议隔离产品是基于隐匿的安全, 相较于网闸, 网闸的安全性更高[4–6].

1.2 网络隔离产品的性能要求

在 2006 版国标《GB/T 20279-2006 信息安全技术网络和终端隔离部件安全技术要求》中并没有对网络隔离产品性能作相关要求, 网络隔离产品也不需要做性能测试, 而在替代其的 2015 版国家标准中, 对于网络隔离产品的性能提出可选要求, 即所有网络隔离产品均需要进行性能测试, 记录产品的性能测试结果, 但是结果不作为产品是否合格的评价结论. 从国家标准的演进和更新换代来看, 网络隔离产品的性能受到了重视, 但是还没有作为产品是否能够通过认证的测试条目.

网络隔离产品和其他安全产品类似, 也涉及到数据的交换, 国家互联网信息办公室网络安全专用产品目录中对网闸产品的性能进行了约束, 通过测试其性能是否满足标准, 在技术层面限制了被测网闸是否能够成为网络安全专用产品, 而且该限制是强制的. 因此网络隔离产品的性能受到越来越多的重视.

2 网络隔离产品性能测试方法研究

本节针对网络安全专用产品和 2015 版国家标准的要求分别设计网络隔离产品的性能测试方法, 对于网络安全专用产品而言, 其性能要求的网络隔离产品特指网闸.

2.1 网络安全专用产品测试方法研究

2.1.1 吞吐量

网络安全专用产品中对网闸性能的第一个要求是吞吐量. 一般的, 吞吐量是指对网络、设备、端口、虚电路或其他设施, 单位时间内成功地传送数据的数量(以比特、字节、分组等测量). 对于网闸来说, 吞吐量是指在没有帧丢失的情况下, 设备能够接收并转发的最大数据速率.

吞吐量与产品的标称值相关, 通常产品的标称值为 10 Gbps(万兆), 1 Gbps(千兆) 和 100 Mbps(百兆), 即在测试时, 测试产品吞吐量与标称值切合程度. 测试吞吐量时, 可以使用软件和硬件两种测试方法, 在使用软件进行测试时, 可以使用 iPerf 软件进行测试, 使用硬件进行测试时, 可以使用 IXIA 的 IxNetwork 模块.

2.1.2 系统延时

网络安全专用产品中对网闸产品性能的第二个要求是系统延时. 一般的, 延时是指从设备接收端口接收到数据包到转发到设备的目的端口之间的时间间隔. 对于网闸来说, 系统延时是指产品一端接收到数据包, 处理数据包 (安全策略、协议剥离等), 摆渡数据包, 传输到对端处理数据包 (协议封装、安全策略) 至发送端口的耗时.

测试延时的时候, 同样可以使用软件和硬件两种测试方法, 在使用软件进行测试时, 使用 iPerf 软件发送数据包并使用 Wireshark 或者 Tcpdump 网络协议分析工具捕获网络数据包. 使用硬件进行测试时, 同样可以使用 IXIA 的 IxNetwork 模块.

2.1.3 软件测试方法

(1) 吞吐量

iPerf 软件是用于主动测量 IP 网络上最大可实现带宽的工具, 因此可以使用其进行产品吞吐量的测试, 在测试时, 选择 2 台性能较好的 PC 机, 此处性能较好指的是不能够低于被测产品标称的吞吐量数值, 如使用千兆的 PC 机去测量万兆产品的性能, 显然是无法测试出吞吐量的实际值的. 选择好 PC 机后, 还需要选择一台时间服务器, 提供 NTP 服务, 为什么需要 NTP 服务器, 下文介绍测试延时指标时会再做说明. 测试拓扑如图 1 所示, 在 PC1 和 PC2 上打开 iPerf 软件并分别运行于服务器和客户端模式, 使用客户端向服务器发送数据包的方式进行产品吞吐量的测试.

(2) 系统延时

iPerf 软件虽具有测试延时抖动等参数的功能, 但是不具有测试延时的功能. 因此测试时使用网络协议分析工具配合, 获取同一个数据包到达接收端口和目标端口的时间, 计算时间差值. 但是使用这种方法时首先要在产品内部设置合适的 MTU 值或者数据包协议剥离、封装的模式, 使数据包不要分片, 即保持输入数

据包和输出数据包的一致性; 其次要保证网闸连接内部安全域主机和连接外部安全域主机的主机时间的一致性, 因此需要用到上文提到的 NTP 服务器做时间同步. 但是经过多次测试, 受网闸内部晶振等影响, 时间无法保持绝对一致, 总会出现 ns 级甚至 ms 级别的误差, 因此在做实验前, 除了进行时间同步, 还需要提前计算时间误差, 在计算延时时, 将时间误差计算在内, 可获得相对精确的延时测试结果.

图 1 iPerf 软件测试拓扑图

2.1.4 硬件测试方法

使用 IXIA 硬件进行测试时, 环境和配置方法较为简单便捷, 开启 IXIA IxNetwork 客户端软件, 选择 RFC 2544 测试模块, 分别进行流配置 (配置端口、IP 地址和传输方向), 协议选择 (选择需要使用的协议, 如 TCP 或者 UDP), 流选项 (字节大小、起始延时等), 开始参数 (延时的计算方式等), 测试参数 (测试时间、测试的轮数等). 测试拓扑如图 1 所示, 设备与 IXIA 使用网线直连, 由 IXIA 分别模拟服务器和客户端进行吞吐量和延时的测试. 测试结束后可由 IXIA 直接得出被测设备的吞吐量和延时.

图 2 IXIA 硬件测试拓扑图

2.2 国标性能测试方法研究

2.2.1 交换速率

一般的, 交换速率又称传输速度, 指单位时间内在数据传输设备传送的比特、字符或消息的平均值. 因此交换速率更加接近于设备实际工作时的传输速度, 即吞吐量测试设备的极限值, 而交换速率测试设备的实际工作值. 交换速率可以以两个指标来衡量, 最大交换速率 (吞吐量) 和实际工作交换速率.

最大交换速率的测试方法, 上节已有介绍, 可以使用软件或者硬件进行测试, 下面简要说明实际工作交换速率的测试方法.

根据网闸实现机制和支持的协议的不同, 网闸的实际工作方式多样. 但是目前网闸基本都支持文件交互或同步 (个别应用于工控领域的网闸不支持文件传输), 因此在测试网闸的实际交换速率的时候, 可以使用传输文件的方式进行测试, 计算整个文件同步完成后, 所消耗的时间, 根据文件大小计算网闸在实际应用环境中的交换速率, 来确定交换速率是否达到国家标准中交换速率大于 1000 Mbps 的要求.

2.2.2 硬件切换时间

因网闸特殊的硬件结构, 如 2.1 节所述, 网闸内部具有切换开关, 用来断开内外部安全域的直接相连, 因此硬件开关的切换速度, 切换时所消耗的时间, 关系到网闸的传输性能, 切换时间可以使用如下方法计算.

网闸内部结构图如图 3 所示, 查阅隔离部件内部缓存大小, 设为 C, 使用上节计算的交换速率, 设为 V, 则切换时间的计算公式为$T=C/V$. 这种计算方法在已计算出交换速率的情况下, 通过查阅隔离部件内部缓存大小的方法计算得出隔离开关在整个打开到闭合结束的时间. 但是这种计算方法并不准确, 误差出现在隔离部件内部缓存大小标称不准确和每次进行数据交换时, 向隔离部件内 (摆渡区) 写入的数据量不可能完全相同. 因此这种计算方式存在的误差较大. 目前国家标准中关于切换时间的性能指标被系统延时取代, 即使用网络安全专用产品的性能指标, 因为该指标包括了硬件切换时间和网闸对数据包的处理所消耗的时间, 更能体现网闸的真实延时性能[7,8].

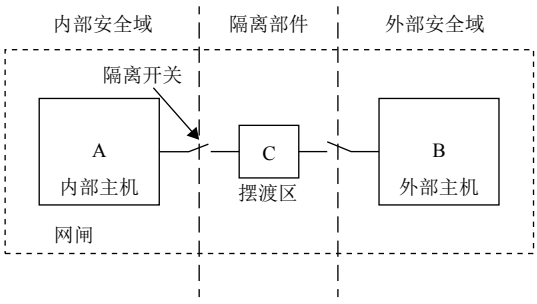

图 3 网闸产品内部结构图

3 性能测试实验

前一章中已经介绍了网闸的性能测试方法, 本章根据上一章介绍的方法对网络安全专用产品中要求的网闸性能进行测试并进行结果分析.

以标称值为千兆的网闸产品为例, 分别使用软件和硬件的测试方法进行吞吐量和系统延时测试.

3.1 软件方法测试

测试拓扑如图 1 所示, 选择 2 台千兆性能的测试 PC(PC1 和 PC2), 均安装 iPerf 软件. 在 PC1 上启用 iPerf 软件并设置为服务器模式, 在 PC2 上启用 iPerf 软件并设置为客户端模式, 使用六类线将两台 PC 直连, 测试 PC 机的最大数据包传输速率. 确认两台 PC 直连数据包传输速率能够到达 1 Gbps, 即能够达到千兆网闸吞吐量的标称值[9,10].

测试步骤如下:

步骤 1. 网闸工作于代理模式, 并配置一条从外到内的单向 UDP 全通策略, 使基于 UDP 的数据流能够正常通过网闸, 而不被网闸阻断 (注: 个别产品需要配置 UDP 源和目的端口);

步骤 2. 对网闸的内部、外部安全域主机 (简称内部主机和外部主机) 进行与 NTP 服务器的校时, 校时结束后, 记录 2 台主机之间的时间误差, 如图 4 所示;

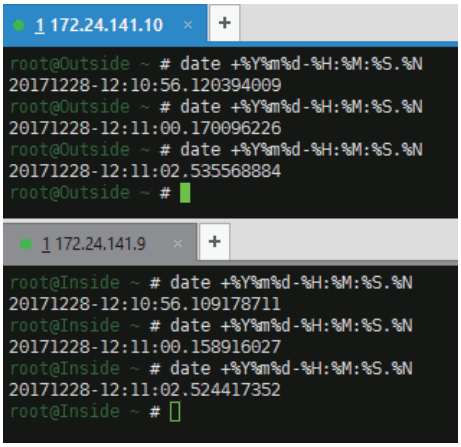

图 4 使用 NTP 校时后的网闸内、外部主机时间

步骤 3. 将网闸串联在 PC1 和 PC2 之间, 并使 PC1 连接网闸内部主机, PC2 连接网闸外部主机, 并在网闸的内部、外部主机上开启流量分析软件 (如 Wireshark 或 Tcpdump);

步骤 4. 在 PC1 上运行 iPerf 服务器指令 iperf -s -u -p 5000 -t 30, 使用 UDP 协议并开启 UDP 的 5000 端口, 每 30 秒统计一次流量;

步骤 5. 在 PC2 上运行 iPerf 客户端指令 iperf -c 192.168.0.1 -u -p 5000 -5 -P 1 -l 1518 -b 1000 M, 连接 192.168.0.1 的服务器, 并以一个线程向服务器的 UDP 5000 端口发送流量带宽为 1000 Mbps, 字节大小为 1518 KB 的数据流;

步骤 6. 重复发送 3 次, 记录服务器端的统计结果, 并求三次的平均值, 如图 5.

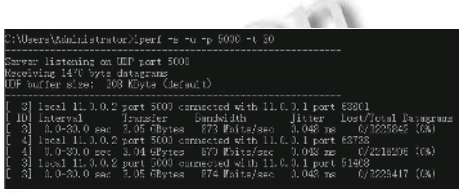

图 5 服务器端的测试结果

通过以上步骤能够测试出该网闸的吞吐量和系统延时, 在计算系统延时的时候, 需要将内、外部主机上获取的对应的数据包时间差再减去内外网主机之间的时间误差.

3.2 硬件方法测试

3.2.1 实验步骤

测试拓扑如图 2 所示, 测试步骤如下:

步骤 1. 网闸工作于代理模式, 并配置一条从外到内的单向 UDP 全通策略, 使基于 UDP 的数据流能够正常通过网闸, 而不被网闸阻断 (注: 个别产品需要配置 UDP 源和目的端口);

步骤 2. 将网闸的内外部主机测试网口与 IXIA 直连, 使用 IxNetwork 配置 IXIA 的测试参数;

步骤 3. 在 IXIA 上选择测试端口, 并配置 IP 地址, 填入网闸的内外网主机地址作为网关地址;

步骤 4. 配置流方向, 将 IXIA 的数据流打向网闸的代理端口, 选择快速测试中的 RFC2544, 吞吐量/延时测试用例, 在用例中进行参数配置, 选择二分法, 使用固定 1518 字节的 UDP 数据包测试吞吐量, 并同时计算延时, 测试三次, 取平均值. 配置界面如图 6 所示, 测试结果如图 7 所示.

由测试结果可以看出, 被测网闸在千兆环境下能够按照线速进行数据包转发, 即千兆速率下未丢包, 但是 L2 层的统计结果却显示 986 Mbps, 小于 1000 Mbps, 是因为 IXIA 在进行发包测试时插入了前导码, 且发包时也具有帧间隙, 导致了统计结果略小.

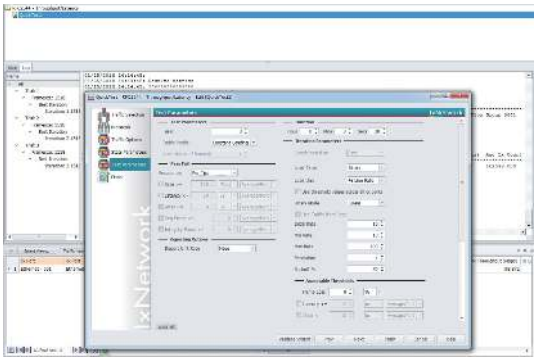

图 6 IXIA IxNetwork 参数配置界面

图 7 测试结果

理论上, 通过使用硬件和软件的测试方法均能够测试出网闸的性能参数, 但是通过测试结果分析, 使用硬件测试的结果更能够体现网闸性能的极限值, 且硬件设备配置过程简单, 可以直接得出实验结果, 系统延时不需要进行计算, 但是在不具有昂贵的硬件设备的情况下, 软件测试方法的测试结果同样在合理范围内.

3.2.2 统计结果及分析

使用硬件测试方法对 2 款百兆网闸、10 款千兆网闸和 2 款万兆网闸的的吞吐量和系统延时分别进行测试, 测试结果的分布如图 8 所示.

本文基于网络安全专用产品目录中对网闸性能的要求和网络隔离产品国家标准中对网闸性能的要求入手, 设计了基于软件和硬件的性能测试方法, 并使用设计的测试方法对网闸的吞吐量和系统延时进行了测试, 证明了测试方法的有效性. 同时, 随机选取了 14 款网闸, 包括 2 台百兆性能、2 台万兆性能和 10 台千兆性能的产品, 对其性能进行了测试, 得出了性能的分布情况和网闸的性能瓶颈.

4 结语

本文基于网络安全专用产品目录中对网闸性能的要求和网络隔离产品国家标准中对网闸性能的要求入手, 设计了基于软件和硬件的性能测试方法, 并使用设计的测试方法对网闸的吞吐量和系统延时进行了测试, 证明了测试方法的有效性. 同时, 随机选取了 14 款网闸, 包括 2 台百兆性能、2 台万兆性能和 10 台千兆性能的产品, 对其性能进行了测试, 得出了性能的分布情况和网闸的性能瓶颈.

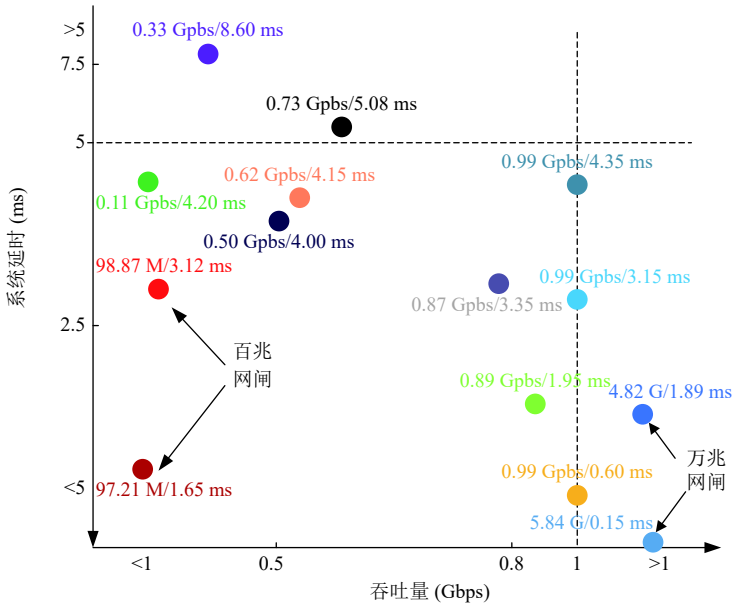

图 8 14 款网闸性能测试结果统计

参考文献

1 国家互联网信息办公室. 关于发布《网络关键设备和网络安全专用产品目录 (第一批)》的公告. 2017 年第 1 号.

2 中华人民共和国国家质量监督检验检疫总局, 中国国家标

准化管理委员会. 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. 北京: 中国标准出版社, 2016.
3 中华人民共和国国家质量监督检验检疫总局, 中国国家标准化管理委员会. GB/T 20277–2015 信息安全技术 网络和终端隔离产品技术评价方法. 北京: 中国标准出版社, 2016.
4 须文波, 胡晋. MIPS 千兆网闸系统实现及其信号完整性设计. 江南大学学报 (自然科学版), 2005, 4(4): 419–422. [doi: 10.3969/j.issn.1671-7147.2005.04.022]
5 寇磊, 周安民, 吴少华. 多用户并发方式的网闸实验系统设计. 四川大学学报 (自然科学版), 2008, 45(3): 544–548. [doi: 10.3969/j.issn.0490-6756.2008.03.020]
6 王锡普, 陈奇. 基于“池”策略的网闸并发连接数提高方法. 计算机工程, 2011, 37(13): 248–250, 264. [doi: 10.3969/j.issn.1000-3428.2011.13.082]
7 曹旭东, 张实. 基于 FPGA 的高速网闸交换卡的设计. 科学技术与工程, 2013, 13(22): 6610–6615. [doi: 10.3969/j.issn.1671-1815.2013.22.048]
8 王樱, 薛滨, 王文奇. 基于 LINUX 网桥实现隔离网闸技术的应用. 河南科技大学学报: 自然科学版, 2008, 29(5): 26–29.
9 傅雷扬, 朱军, 饶元. 一种跨网闸数据传输系统的设计与实现. 计算机与数字工程, 2016, 44(10): 1996–2000. [doi: 10.3969/j.issn.1672-9722.2016.10.028]
10 寇雅楠, 李增智, 王建国, 等. 计算机软件测试研究. 计算机工程与应用, 2002, (10): 103–105. [doi: 10.3321/j.issn:1002-8331.2002.10.034]