《互联网周刊》2010 年第 17 期 总第 479 期

UTM 与 NGFW 的新瓶旧酒

清华大学信息技术研究院 李军

近年来，国际上的一些市场分析公司风格越来越像媒体,有股语不惊人死不休的味道。2003 年 6 月，Gartner 的副总裁、分析师 Richard Stiennon 发表的《Intrusion Detection is Dead - Long Live Intrusion Prevention（入侵检测寿终正寝，入侵防御万古长青）》，就是一例。不仅如此，著名的市场分析公司并不总是意见相同，常常让人无法适从。好在“实践是检验真理的唯一标准”，至少市场预测的结果是可以随着时间推移去伪存真的。

（一）

近年来，网络安全市场波澜不惊，少有 Netscreen 从 1997 年初创到 2003 年上市再到 2005 年并入 Juniper 那一段时间创业公司层出不穷、公司上市一浪高过一浪的景象。事实上，Netscreen 被收购的发生，意味着以网络安全为网络智能的核心而一统网络设备市场天下的梦想破灭，网络安全设备厂商从此偏安一隅，新兴网络安全市场也往往被传统的路由交换“巨头”们通过并购蚕食，难以成为独立产品市场。端点安全（End-point Security）、信息或数据泄露防御（ILP：Information Leakage Prevention 或 DLP：Data Leakage Prevention）[1]、网络准入控制（NAC：Network Admission Control）都是这样的例子、这般的下场。在以新兴产品形态成为独立市场之前,其中的领头企业就几乎被路由交换大厂并购一空。

至今存活下来的独立网络安全产品公司，主要有两类：一类是从防病毒起家的，逐步借助优势把握恶意软件（malware）防控和相关市场，但有些也在暗度陈仓，例如 Symantec 通过并购进入了存储市场[2]；另一类是传统的防火墙、入侵检测和防御（IDS：Intrusion Detection System 和 IPS：Intrusion Prevention System）厂商，虽然有些老牌厂商如 WatchGuard 和 SonicWall 已经被私募股权投资拿下，不再是上市公司，但 CheckPoint 还算硬朗，SourceFire 也尚活跃，

[1] 也有人将之与 IPS 对应，称为外泄防御系统（EPS：Extrusion Prevention System）。国内也有将其与防火墙对应，称之为“防水墙”的。

[2] 存储与数据安全的合流还有 EMC 收购 RSA，NetApp 收购 Docru 等案例。

而且无论中美，零星还会有 Fortinet 和启明星辰这样的公司上市，也还有 Palo Alto Networks 和山石等创业公司出现。

在防病毒等恶意软件方面，目前路由交换巨贾们还没有太多介入，基本上是采取与传统防病毒厂商合作的策略，但防火墙、IDS/IPS、虚拟专用网（VPN：Virtual Private Network）以及由此衍生出来的统一威胁管理（UTM，Unified Threat Management），则是 Cisco、华为/华赛、Juniper 等的拿手好戏，不会让专营网络安全的厂商专美于前。这就使得专业网络安全厂商特别是后起之秀们必须想方设法发现用户对网络安全硬件设备的新需求，在技术创新上抢得先机，在产品特色上占据主动。而在这方面，最好的办法就是让市场分析公司认识到新型、特色产品的价值，充当吹鼓手。市场分析公司当然也不愿错失“发现新大陆”的机会，对于“定义”一个新产品类型、描绘一个新市场方向更是乐此不彼，从而确实对市场发展发挥了推波助澜的巨大作用。这便形成了一个“共谋”的生态。

（二）

作为将防火墙、VPN、IPS 以及网关防病毒等功能结合于一体的网络安全设备，UTM 最初是针对中小企业（SMB：Small and Medium-sized Business）[3]客户的需求提出的。2004 年 9 月，IDC 最早提出 UTM 的概念，认为它作为一种新的产品形态正在形成网络安全产业中的一个新兴细分市场，并将于 2008 年以近 20 亿美元的市场份额超过防火墙/VPN [1]。到了 2008 年，IDC 宣称 UTM 市场规模在 2007 年超过了 10 亿美元，并预期将在 2012 年达到整个网络安全市场的 33.6%。据另一家市场分析公司 Frost & Sullivan 最近发布的报告，UTM 的全球市场规模在 2009 年达到了 19.7 亿美元，并有望于 2016 年达到 70 亿美元左右。

UTM 产品符合中小企业对降低设备和管理成本的需求，也在一定程度上提供了分立产品无法做到的防御抗击综合性攻击手段的能力，获得了巨大的市场成功，成为近年来成长最快的网络安全设备类别。然而，对于大型企业来说，一般 UTM 设备对相关安全功能的深度整合不够，集成优势发挥不足，同时性能瓶颈也是非常突出的问题。这种情况也引发了很多争论，正如当年国内关于防火墙的“胖”、“瘦”之争，为下一代防火墙到底是应该更突出功能集成(因包含很多功

[3] 各国定义或约定俗成不尽相同，在美国通常指 5 百人以下，我国一般指 2 千人以下，且对销售和资产金额有一定数目要求。

能而增“胖”）还是更强调性能突破(为保证处理速度而“瘦”身）而各执一词。对此，笔者认为性能和功能从来就是一个矛盾的两个方面，不能试图用一种软硬件体系结构解决所有的问题，并在 2003 年就曾经提出：最有可能出现的局面是“矮胖子” 和“高瘦子”共存。

所谓“矮胖子”，多数会是基于 CPU 加 Linux 的计算平台，服务于低端市场。因为目前 CPU 的处理能力已经大大超过低端底层网络处理的需求，完全可以利用其空闲时间进行更多应用代理、内容过滤等协议和数据处理。而高瘦子则指高端产品，它们主要还会是综合应用 CPU、NPU(网络处理器)、ASIC 以及加速数据加密和协议分析等特定功能的协处理芯片，构成高速可靠的安全计算平台。这样一个“矮胖子” 和“高瘦子” 并存的产品形态分布不但与现有软硬件计算技术的水平相适应，而且也与实际需要相吻合，正所谓“环肥燕瘦总相宜”，而且胖瘦、高矮的分界线也是随着时间而变的。通常的情况是，核心安全区域一般流量较小，但对应用层安全要求较高，而公共性越强的网络节点对性能要求越高，却并不一定要求防病毒、防垃圾等应用层过滤[2]。

（三）

有趣的是，同是著名市场分析公司的 Gartner 一直对一些厂商借助 UTM 的人气将其推向大型企业不敢苟同，甚至在 2005 年就在正式发表的研究报告中明确宣称“（大型）企业 UTM 根本就不存在”。事实上，Gartner 一直宁愿将这类产品称为“中小企业多功能防火墙”，而对于“UTM”这个说法总是很不情愿。Gartner 的副总裁、分析师 Greg Young 说，Gartner 既没有发现（大型）企业转而使用 UTM， 也不认为这会在不远的将来发生。相反，他们注意到 UTM 的现有用户企业一旦成长到 750 人左右，就会改用单点（分立）设备，而且不再回头。

2009 年 12 月，Gartner 的 John Pescatore 和 Greg Young 提出了 NGFW，即下一代防火墙（Next Generation FireWall）的概念[3]，与笔者 2003 年提出的“高瘦子”说法甚为相像。相对 IDC 于 2004 年提出的类似“矮胖子”的中小企业级 UTM 而言，NGFW 也主要是在提高性能要求的前提下，去掉了在高端网络安全设备部署中很少需要的防病毒等通常要在“应用层”和“文件级”进行处理的安全功能，保留了在网包（packet）和网流（flow，或更细分的会话，session）层处理的网包过滤、状态检测(Stateful Inspection)和深度检测(Deep Inspection)

等核心技术环节，并对通过安全功能深度集成以更好抵御 botnet 等新型攻击、提供对 P2P 等应用的控制提出了更高要求。他们预测，到 2014 年底，NGFW 将占有防火墙（以及 IPS）市场的 60%。

其实，无论是“矮胖子”UTM，还是“高瘦子”NGFW，真正革命性技术突破并不多，可以说还都主要是新瓶装旧酒。当然，网包过滤、状态检测，特别是深度检测这些“旧酒”还是有很多可以提高和发展的余地。例如，近来学术界发表的成果已将网包过滤（分类）的性能推进到了单芯片（FPGA）100Gbps，而深度检测的单芯片（网络处理器）性能也超过了 10Gbps。又如，在协议分析和流量管理，以及适应多核、并行处理所需的创新等方面，也都有不少新的研究成果。而“新瓶”是否成功，还是要看市场需求是否把握得准，特别是在面临云计算带来互联网结构巨大变化的今天。

（四）

无论是 UTM 还是 NGFW，面临的重要问题都是如何做到功能深度集成和如何达到性能大幅提升。虽然近年来各大厂商在产品研发中都在不断有所推进，但在一些关键技术方面，例如高速正则表达式匹配，尚待算法或芯片技术的重大突破。不过，网络应用的普及和移动计算的发展正在使得信息安全成为焦点，这将大大推动相关技术的进步。最近发生的 Tektronix 对 Arbor Networks 的收购和刚刚宣布的 Intel 对 McAfee 的收购就是产业界提供的两个新鲜例证。另外，最近嵌入式处理器测评协会（EEMBC：Embedded Microprocessor Benchmark Consortium）开始了称为 DPIBench 的标准测试起草工作。缺乏公正、完整的测评体系，使得高性能安全网关设备市场上很多不实或刻意以偏盖全市场宣传的存在成为可能，不但给用户选择和使用带来困惑，而且减低了技术创新的压力和动力。DPIBench 试图建立一个业界普遍接受的标准测评体系，以便比较系统和芯片的深度检测性能，如能成功，将对技术进步和产业发展大有裨益。

在新的技术突破到来之前，市场上的选择大多只会是新瓶装旧酒。但我们完全有理由期待全新技术的出现。

参考文献：

[1] Charles J. Kolodgy, Worldwide Threat Management Security

Appliances 2004-2008 Forecast and 2003 Vendor Shares: The Rise of the Unified Threat Management Security Appliance, IDC report #31840, 2004

[2]李军，第三代安全网关：中国安全产业新机遇，《互联网周刊》2003 年第 43 期，总第 253 期，2003 年

[3] John Pescatore and Greg Young，Defining the Next-Generation Firewall，Gartner, Inc. Publication ID Number: G00171540, 2009