《互联网周刊》2003 年第 43 期 总第 253 期

第三代安全网关：中国安全产业新机遇

清华大学信息技术研究院 李军

就像国家之间有海关、防疫和边防检查站，地区之间(如美国加州和内华达州之间)有农业检查站，要害部门有门卫一样，网络安全中应用最广泛的产品首当部署在网络边界(edge) 上的安全网关(security gateway) 。安全网关通常包括,但不仅限于,防火墙、VPN(虚拟专用网) 网关 、NIDS(网络入侵检测系统) 和安全路由器等。一些基于高层网络协议的交换机和内容过滤设备，也都在一定程度上扮演着安全网关的角色。

安全网关走过的历程

伴随着互联网的诞生和发展，由不同网络安全要求和用户权限级别划分的网络区域(security zone) 对边界控制和保护的要求不断增高，网络攻击和滥用等问题日益突出，安全网关的功能和性能也不断增强，大致经历了两代产品的研发和应用，正在迈入第三代。

最初的安全网关很自然地由附加在边界路由器上的简单 ACL(进出控制表) 构成。当时的 ACL 大多只是在第 3 层网络协议(网络层，network layer) 上根据来源地址和目的地址对途经边界的网包(packet，又译为分组) 加以转发或丢弃，从而构成了*网包过滤防火墙*，在一定程度上保护不同网络区域或网段(network segment) 之间连接的安全性。经历了上个世纪 90 年代初一些厂家的*应用代理防火墙*尝试之后，第一代作为独立产品的安全网关当属以 CheckPoint 公司相关产品为代表的第一代防火墙。

第一代安全网关是以分立式为特征的软件防火墙产品。这一代产品在网包过滤防火墙的基础上，引入了在第 4 层网络协议(传输层，transport layer) 上通过状态检查增强安全性、提高吞吐率的*状态检测防火墙*技术，但在形态上大多还是单独安装在服务器上的软件产品。

到了上个世纪 90 年代中，以 NetScreen 为代表的硬件安全网关厂家崛起，并在 90 年代末逐渐形成了第二代安全网关在市场上的相对优势。这一代产品的特征是集成了防火墙、VPN 网关和一些防攻击功能，并以 ASIC(专用芯片) 为这

几部分的技术实现基础，从而大大提高了安全网关的吞吐能力，适应了当时局域网环境从十兆(10 Mbps) 向百兆(100 Mbps) 迅速升级、千兆(1 Gbps) 需求开始形成规模的市场发展态势。

在第二代安全网关厂家中，比较典型的还有 SonicWall 及其收购的 RapidStream、WatchGuard 及其收购的 RedCreek。不能不提及的当然还有携品牌和渠道优势而在市场占有率上一家独大的 Cisco 及其收购的 Network Translation。不过，至少在初期，Cisco 以及与 CheckPoint 合作的 Nokia 从技术实现上更接近第一代安全网关，只是形态上以硬件产品出现而已。

安全网关面临的挑战

随着网络带宽的迅速增加和网络应用的日益丰富，安全网关的产业竞争也像奥林匹克竞赛一样面临着更高更快的挑战：市场呼唤着功能更高更强、性能更快更稳的安全网关产品。一方面，病毒、垃圾以及混合式攻击成为网络安全最为突出的问题，以隐匿于内容等方式出现的网络攻击模式也越来越复杂；另一方面，随着网络流量的增加和安全检查负荷的加重，安全网关始终是高速网络中的瓶颈，滞后于高端路由器、交换机的性能水平。

针对日益增长的性能和功能需求，产业界在硬件和软件上不断有所突破，但对市场和技术发展的方向也出现很多争论。前一段国内业界就有“胖”“瘦”防火墙之争，为下一代防火墙到底是应该更突出功能集成(因包含很多功能而增“胖”) 还是更强调性能突破(为保证处理速度而“瘦”身) 而争论不休。其实，性能和功能从来就是一个矛盾的两个方面。例如，应用代理防火墙尽管安全性很好，但 10 多年前却因为当时 CPU 处理能力不够而几乎被舍弃，存活下来的产品屈指可数。现在 CPU 处理能力早已今非昔比，应用代理防火墙技术也浴火重生，越来越多地被具有防病毒等功能的安全网关所采用。又如，仅用 CPU 作为支撑的硬件平台，无论是以服务器上安装软件还是专用硬件系统的产品形态出现，最初都不能满足多功能集成的性能要求。如今，CPU 处理能力和多处理器结构已经完全可以承担百兆级多功能线速的负荷。这既是第一代安全网关以分立式面目出现的根本原因，也是目前低端防火墙摆脱 ASIC，回归 CPU 架构的内在驱动。

因此，不能试图用一种软硬件体系结构解决所有的问题。安全网关的产品形

态也一定是随着软硬件计算技术的发展而变化的。笔者认为，近期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，服务于百兆为主的低端市场。因为目前 CPU 的处理能力已经大大超过网包处理的需求，完全可以利用其空闲时间进行更多应用代理、内容过滤等网络和数据处理。这种在线速条件下实现多层、各种网关处理功能的产品正是第三代安全网关。而高瘦子则指万兆(10 Gbps)或近万兆带宽的高端产品，它们主要还会是综合应用 CPU、NPU(网络处理器) 、ASIC 以及各种加密和协议分析芯片，构成高速可靠的安全计算平台。换句话说，基本上还是第二代安全网关向更高带宽的延伸。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 ”。因为通常的情况是，核心安全区域一般流量较小，但对应用层安全要求较高。反之，公共性越强的网络节点对性能要求越高，但并不一定要求防病毒、防垃圾等应用层过滤。当然，在高速节点上需要进行内容过滤的情况也有，但终归不是市场主流的企业级产品需求。

在百兆低端和千兆高端之间，千兆或近千兆吞吐能力的产品则会是多 CPU、CPU 与 NPU 结合、CPU 与 ASIC 结合等多种形式并存。正如历史上很多产业在发展阶段的技术实现都呈螺旋式上升的一般规律，安全网关产品也不例外。市场需求和技术进步决定了主流产品的研发路线。千兆或近千兆带宽产品正在从过去的高端逐步过渡为现在的中端。千兆层次上的第三代安全网关产品所面对的性能和功能要求，用现有的安全网关产品体系结构较为难以满足，但也是最有可能推陈出新的。NPU 的日臻成熟解决了千兆以至多千兆线速的网包处理能力，完全可以满足防火墙、VPN 和 NIDS 的网络处理要求。

总之，集成多层各种网关处理功能并不是一个新概念，但是只有当硬件或算法发展到相应阶段才能梦想成真。集成的趋势在低端上已经很明显了，但在中端以至高端上还有待于系统和芯片技术的突破。CPU 的不断提速和多 CPU 体系的普及提供了内容过滤、防病毒和防垃圾等应用所需的数据处理能力。然而，尽管 Intel 计划针对中端和多口低端市场推出结合多种处理功能于一体的芯片(包括 1 个兆赫左右的 CPU 核 Xscale 、4 个兆赫左右的微处理引擎、2 个用于加解密等功能的专用引擎) ，但目前在 90 纳米芯片生产技术下将真正高性能 CPU 与 NPU

集成为一个芯片还几乎是不可能的。就连 Intel 的专家也认为，即使在 60 纳米芯片生产技术下这一水平的集成也不太可能。因此，真正的挑战在于实现 CPU 与 NPU 高速“ 无缝 ”互联的硬件平台，而其核心则是 CPU 与 NPU 相通的总线。

安全网关崭新的机遇

回顾安全网关的发展历程，分析安全网关所面临的挑战，我们可以看到中国安全网关产品研发所获得的重大机遇。

首先，国内市场目前需求量最大的是百兆和百兆以下的低端产品。因为国内安全网关产品研发起步相对较晚，ASIC 研发能力又相对较弱，所以多数产品都是基于 PC 硬件平台和 Linux 软件平台开发的，而这恰好与低端安全网关产品回归通用 CPU 加 Linux 体系的潮流相符合。这使得国内安全网关厂商在以 Linux 为基础的低端安全网关产品研发上，特别是防火墙和 NIDS 以及安全网关集中管理平台等方面，积累了相当的经验和人才，从而占有一定优势。将这一优势与国内 PC 厂家的产量和成本优势结合起来，在产品定位上更好地与国际市场的需求接轨，将有可能继中国家电形成较强出口能力之后，在中国网络设备逐渐形成一定出口能力的进程中中发挥作用。

以目前的情况看，国内厂家在防火墙与 NIDS 的集成上走得较快。在 NAI 收购 Intruvert、NetScreen 兼并 OneSecure，处于产品整合阶段之时，国内一些基于 CPU 加 Linux 平台的研发型企业借助通用硬件和开放软件平台灵活易变的优势，已经推出集成了防火墙、VPN 与 NIDS 的安全网关产品。这些产品只要能够在吞吐率和稳定性上尽快得到提高，就可以在 NetScreen 等国外公司新一轮集成产品推出之际立于不败之地。不过，由于国内防病毒厂家与安全网关厂家合作不多，防垃圾厂家还处在起步阶段，国内安全网关厂商在应用集成方面有一定困难，面临挑战。Symantec、NAI 等厂商以应用层安全网关的优势和收购防火墙、NIDS 公司的战略，正在积极准备下一波应用集成安全网关。ServGate 与 NAI 合作已经推出了集防火墙、VPN 和防病毒、防垃圾等应用代理功能于一体的模块化集成安全网关。NetScreen 虽然限于 ASIC 体系尚未全线推出集成的防病毒、防垃圾功能，但也在强化与 TrendMicro 的合作，并已在新款低端产品上实现了集成的防病毒功能。TrendMicro 最近的调查显示，60%的商业用户相信边界网关是病毒

防范的最有效位置。国内安全网关厂商应该尽快加强与国内外防病毒、防垃圾、XML 过滤等应用层安全厂家的合作，在应用集成方面有所作为。

其次，国内市场对千兆产品的需求增长相对较快。同样因为国内复杂 ASIC 的研发能力较弱，而接触国外以 ServGate 等公司为代表的基于 NPU 而不是 ASIC 的千兆安全网关产品较早，使得国内很多厂家都选择了基于 NPU 开发千兆产品的技术路线，形成了一定的群体优势，造成了著名国际 NPU 厂商对中国 NPU 市场的高度重视和大量投入。这使得国内网络设备厂家有可能在整体上形成基于 NPU 的系统研发优势，率先形成基于通用 NPU 的软硬件平台，在特定意义上领导国际上开放网络设备平台的潮流。NPU 作为适应于网络处理的可编程通用芯片，相对于 ASIC 明显具有研发周期短、成本低，且软件共享性和系统扩展性好等突出优点。正如当年 Intel 和微软造就了 IBM 兼容 PC 机从而带动了 PC 的大众化普及一样，一个开放网络设备平台将有很大的潜力。

正如信息产业部在 2003 年电子信息产业基金招标文件中指出的，“ 目前在国内市场上国外的千兆防火墙产品已占据主流地位，因此开发高性能、高稳定性具有自主知识产权的千兆线速防火墙系统，对于适应与满足国家信息安全建设要求，建设我国自主知识产权的信息保障基础设施具有重要的战略意义 ”。目前国内市场上的国产千兆防火墙，大多是基于 CPU 和 PCI 总线的，属于第一代防火墙，硬件体系结构落后，致使产品性能低下，多数 “ 只有千兆接口，没有千兆能力 ”，成为千兆网瓶颈，完全无法适应高流量需求。可喜的是，基于 NPU 的国产千兆防火墙已经出现。今年，中科网威、联想先后推出了基于 NPU 的千兆线速安全网关产品，据悉紫光比威、华为等公司近期也将陆续推出基于 NPU 的、具有自主知识产权的安全网关新产品。这些产品分别应用了目前最流行的 Intel、Broadcom、IBM 等厂家的 NPU。

正如信息产业部指出的，“ 推出性价比高、实用性好、市场竞争力强、技术先进、具有自主知识产权的千兆线速防火墙系统，并达到规模化生产要求 ”，从而 “ 在高端市场上逐步占据主导地位，满足国内迅速增长的网络安全产品市场需求，为建设我国信息安全框架提供基础产品，更好地保障我国网络信息安全”。只有做到了这一点，才能创造由政府通过政策措施保护国家安全的基础，解决目前鱼目混珠(用国外产品贴牌或 OEM 进入政府网络)的问题。

与此同时，应当重视将相关成果催化成为开放平台，推动硬件设计和底层软件以模块化的参考系统方式有偿转让，以利更多厂家增加功能、开发产品。这样做的好处是能够鼓励国内厂家参与第三代安全网关的群体突破，在千兆线速安全网关上形成竞争，真正达到国内自主开发千兆线速安全网关的大规模产业化。也只有这样做，才能解决个体突破所带来的对国外少数 NPU 厂家的依赖，并鼓励国内对 NPU 本身的研发和 ASIC 的发展。（文/清华大学信息技术研究院 李军）

参考文献：

中华人民共和国信息产业部,电子信息产业发展基金招标项目千兆线速防火墙系统规范书，2003 年 10 月

Mike Rothman, *3G Firewalls: Is Bigger Better?* The Optical Oracle, Vol. 2, No. 10, Oct. 2002

John Daly, Roseann Day, and Charles Kolodgy, Security at Wire Speeds, IDC Report #02C3446, Oct. 2002