《信息网络安全》2004 年第 7 期 总第 43 期

防火墙上台阶：安全网关多层过滤技术的走向

清华大学信息技术研究院 李军

防火墙走过了第一代和第二代，正在七嘴八舌、众说纷纭中坚定地逐步走向第三代。然而，究竟什么是第三代防火墙的特征，第三代防火墙又将为我们带来什么？更高的性能，更多的功能是永恒的主题自不用说。但什么样的硬件和算法可以让我们获得在更高集成度下的更高吞吐率指标，什么样的安全应用适于有机地内置于网关设备？这些都是需要回答的问题。

4 层以下的戏演完了吗？

如果说国内关于防火墙发展的“ 胖 ”、“ 瘦 ”或“ 发胖 ”、“ 发威 ”之争还是在增加功能和提高性能之间权衡的话，国外企业在这方面则争论很少、行动很多，各自根据自己对市场需求、自身定位和技术优势的分析，不断增强产品在带宽和服务上的竞争力。国内产品受技术手段局限，“ 瘦 ”的都不够快，“ 胖 ”了就更跑不动了，国外则是从市场出发，在竞争中健身，靠健身来竞争。

事实上，业界虽然把“ 应用层防火墙 ”或“ 7 层防火墙 ”炒得很热，却并不意味着 OSI 协议架构 4 层（含第 4 层）以下已经没有新戏可唱了。NetScreen 创始人之一、首席战略官邓锋在私下和公开场合多次表述了这样的理念，即路由器作为网络智能中心（intelligent center）的时代正在成为过去，以防火墙为代表的安全网关将取而代之。细心的市场分析家可以看到，NetScreen 作为全球硬件安全网关龙头厂商，早在几年前就已染指路由，意在使路由成为安全网关中的“ 大路货 ”功能，并用集成了路由功能的防火墙取代（美而言之“ 省略 ”）Cisco 路由器。最近 NetScreen 被 Juniper 用 40 亿左右美金收购的举措，更证明了两家公司真正的对手其实都是 Cisco。

除了 2 层的 VLAN、3 层的路由和网包（packet,又译为分组）过滤、4 层的状态检测（stateful inspection）之外，从智能网关的角度来看，还有很多其它功能可以集成或完善。比如已经普遍与防火墙一同集成于安全网关的 VPN，以及越来越多集成于安全网关的入侵（intrusion）/攻击（attack）监测和防护、

QoS 和基于协议/服务的负载均衡等。

入侵和攻击常被归为一个大类。目前行之有效的主要还是针对洪泛（flooding）类型 DOS 的基于统计的攻击监测和防护，和基于已知攻击特征的模式匹配的入侵监测和防护。虽然这些方法象现行的防病毒技术一样，难以抵御新型攻击，但毕竟可以挡住多数攻击，如果反应快速往往还可以防止新型攻击大规模爆发。攻击防范中的部分处理，特别是基于统计的部分和基于协议分析的部分，就是在相应的 3 层和 4 层进行的。

一些访问控制需要处理的新的协议，以及某些基于 IP 地址及 DNS 的高速 URL 过滤，很自然地丰富了 4 层及 4 层以下处理的内容。一些相对较新的功能，如 4 层路由或基于服务（4 层协议端口）的负载均衡，也给 4 层及 4 层以下处理的发展开拓了空间。象 DDOS 这类难题，在单一网关上是很难解决的，必须由包括网关在内的外网分级分布式系统协调解决，但至少也需要安全网关具有相应的功能来参与。同样，对付蠕虫等可能通过便携电脑或无线接入等绕过防火墙而泛滥的问题，可以尝试由包括网关在内的内网网络与系统安全体系全面互动解决，当然也需要安全网关具有相应的功能来参与。

7 层的新戏各有各的版本

虽然在防火墙早期发展过程中出现过“应用代理（application proxies）防火墙”，但因为当初性能较差、覆盖较窄，一直没有成为主流。虽然个别产品如 Raptor 和 Gauntlet 一直生存了下来，大体上也是旧瓶装新酒。防火墙技术总体上还走过了从网包过滤到状态检测（实为会话过滤，session filtering）再到今天的内容过滤（content filtering）的历程。如今的内容过滤虽然因为用到了很多应用代理技术而时常被称为应用过滤（application filtering），但已是建立在更高性能硬件平台和较为成熟的 4 层及以下网包处理基础上的。

当然，内容过滤在概念上包含了涉及网包的 TCP/IP 包头（header）之后的信息（亦即 4 层的负荷，payload）的各种处理。在这方面，一些厂家纷纷提出了各自不同的概念。如 Juniper－NetScreen 等从 IDS 业界继承下来的“深度检测（Deep Inspection，DI）”和最早提出安全网关概念的 ServGate 的“全上下文检查（Full Context Inspection, FCI）”等等。

Juniper－NetScreen 较早着手于将 IDS、IPS 集成于安全网关，并期望通过兼并 OneSecure 来加速实现这一战略。将路由和攻击防范集成于安全网关，对于专用芯片设计能力强，以性能卓越见长的 Juniper－NetScreen 来说是非常自然的技术、产品和市场拓展。Juniper－NetScreen 将基于硬件网关的安全防护从低到高分类为网包级、会话级、应用级和文件级。级别越高需要处理的信息越复杂，因而通常速度也越慢。

深度检测可以在逐个网包上进行，但并不象有些资料所述那样局限于深度网包检测（Deep Packet Inspection, DPI）。这正如将状态检测称为状态网包检测同样会引起误解。逻辑上，深度检测包括所有对 7 层协议应用消息（application message）的过滤。它首先将网络流量按照不同的 7 层协议分流（flow），并利用启发信息分析来检查可能的异常，从而屏蔽一些诸如“缓存溢出（buffer overflow）”等攻击；它随后在应用消息的特定服务域（service fields）中针对攻击特征进行模式匹配，以剔除恶意的企图。这些操作在需要时会先行将相关网包缓存，再通过 IP“去碎片化（defragment）”和 TCP“重新组装（reassemble）”，以获得完整的应用消息。从上述介绍可以看出，正如状态检测保持甚至代理 4 层网络协议状态一样，深度检测实际上需要在一定程度上保持 7 层的应用协议状态，从而执行协议分析、分散匹配负担。

以防病毒著称的网络安全公司 Symantec 和 Network Associate 通过并购防火墙、IDS/IPS 逐渐形成了较为完整的安全网关产品线。Juniper－NetScreen 和 ServGate 分别通过与 TrendMicro 和 Network Associate（McAfee 品牌）的合作，将优异品牌的防病毒引擎集成到安全网关中，并利用他们的快速反应团队获得杰出的病毒特征库更新服务。这两个方向的努力，正在促成防病毒、防垃圾等产品演变为融入安全网关的功能。不过，防病毒和防垃圾的引入，不可避免地会带来安全网关在处理相应网络流量时的延迟。这种延迟源于防病毒等对于文件扫描的依赖，对电子邮件的用户体验影响不大，但对于网页浏览则可能会有察觉得到的影响。尽管个别厂家声称做到了流式（streaming）病毒处理，但尚未见到有说服力的文献因而值得怀疑，因为即使做得到流式扫描也做不到清理、隔离或删除。转发出去的网包是收不回来的，而现有的众多应用协议本身也不保证客户端会有回溯操作。

另外，一些专攻应用层安全网关的企业最近也很受关注，例如 F5 刚刚收购了 MagniFire，而 Sanctum 和 Teros 等同类初创公司也很活跃。这些公司在应用层协议过滤（特别是 HTTP 协议分析或所谓的“ 80 口防护 ”）方面的研发独具特色。

Web 服务将会推动新的 7 层努力

安全网关正在变得越来越“ 聪明 ”，或者说越来越具有“ 高级 ”智能。从原本只能处理 3 层协议（网包过滤），到可以处理 4 层协议（状态检测），进而处理 7 层协议（深度检测），一步步上台阶直到内容检测，实现全层过滤（All Layer Firewalling），并形成全面防护系统（Total Protection System, TPS）。这方面的挑战包括动态代理各种 IM（instant messaging）服务以及 SIP 协议等。

新兴的基于 XML 的 SOAP 等相关协议的 Web 服务，可以把不同来源的数据按照不同应用的要求动态构建成文本，正在迅速成为政府（government, G）、商家(business, B)和用户(customer, C)之间（G2B，B2B，G2C，B2C 等）信息表述和交换的公共方式，使得集成的业务流程成为可能。这就要求安全网关能够解析、分析、甚至过滤 XML 网流。DataPower 和 Forum Systems 等初创公司推出的 XML 防火墙正是看好这一市场需求和前景所做出的努力。相信一些著名网络安全厂商也在密切关注这一方向，加大人才和技术储备，伺机而动。著名市场研究公司 Gartner 的安全分析师 John Pescatore 认为，“ 三年之间，所有边界防火墙（edge firewall）都将象处理其它连接（connection）一样，处理 Web 服务连接 ”。

有趣的是，作为 XML Web 服务基础的 SOAP 的最初设计目标之一，恰恰是成为一个服务器之间容易穿过防火墙的协议。XML 防火墙的核心是 XML 解析（parsing）和 SOAP 服务，主要功能包括 XPath 确认（identification）、模式验证（schema validation）、加密和解密、数字签名的签署（signing）和核实（verification）等，其中涉及到 IETF 和 W3C 联合工作组制定的 XML 加密和 XML 签名标准和以它们为基础的 WS（Web 服务）安全标准（包括 WS 加密和 WS 签名），以及 SAML（安全声明标记语言，security assertion markup language）和 XKMS（XML 密钥管理系统，XML key management system）等。

相对于基于 IP 的 IPSec VPN 或基于 TCP 的 SSL VPN 而言，XML 加密或 WS 加

密不再只是 3 层或 4 层上的“ 隧道式 ”保密方式，而是可以有选择性地对整个文本、逻辑元组（element group）或数据单元(individual element)加密。不过，从一些已发表和未发表的数据可以看到，加密和解密似乎并不是 XML 防火墙性能的瓶颈，而且可以使用硬件加速。目前最棘手的是要提高 XML 解析的性能指标。对现有 XML 防火墙的测试表明，即使不使用加密和签名，XML 防火墙每秒最多可以处理不超过 300 消息。

性能提高的挑战是应用层处理所面临的共同问题：防病毒、防垃圾，以致 XML 防火墙。例如，NAI－McAfee 的防病毒网关每秒最多也只能处理几十个电子邮件，2MB 而已。应用层安全网关功能的发展呼唤着新的软硬件解决方案。象 Tarari 这样专门从事内容过滤（特别是 XML 处理）芯片设计的厂商将在短期内增多并大有用武之地。

总之，安全功能在 OSI 协议架构单层上的集成正在完成，多层间的集成方兴未艾，并需要有新的硬件平台和软件实现来突破性能瓶颈。

参考文献：

Frederic Avolio, “ Firewalls and Internet Security, the Second Hundred (Internet) Years, ” Internet Protocol Journal, Cisco Systems, Jun. 1999

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

Juan Pablo Pereira, “ Comparison of Firewall, Intrusion Prevention and Antivirus Technologies, ” White Paper, Juniper Networks

Ying-Dar Lin, Huan-YunWei, and Shao-Tang Yu, “ Building an Integrated Security Gateway: Mechanisms, Performance Evaluation, Implementation, and Research Issues ”, *IEEE Communication Surveys and Tutorials*, Vol. 4, No. 1, third quarter, 2002.