

防火墙、UTM 产品 OEM 第三方产品或嵌入第三方反病毒引擎的利弊分析

皓月

反病毒是信息安全体系中非常特殊的领域，由于其对抗的密度和强度，对资源、对基础依赖的程度远高于其他多数安全领域，因此是多数安全厂商不愿意半路杀入的原因。就连 Cisco 这样的巨无霸企业在推出自防御网络中也是与 trendmicro(趋势)携手，而微软则采用直接购买其他反病毒企业的方法。

正因如此，无论是国内的传统防火墙厂商（，抑或是新兴的 UTM（统一威胁管理厂商）为了即扩展反病毒能力，又不承担庞大的病毒引擎研发分析成本，都在其安全产品中不约而同的嵌入了来自于第三方反病毒厂商的引擎；前者多以新型防火墙为主营业务，后者则以新兴 UTM 架构为主打，市场上一时间风生水起，一片叫好之声；甚至就连长久以来被人所指责的“网络病毒检测过滤性能瓶颈”也随着 ASIC 专用芯片、多核 NP 等硬件技术的应用而号称“已经解决”。

根据比较可靠的资料分析，国内比较有代表性的安全厂商为了迅速扩展产品线，或者提升产品能力，分别采用过 OEM 国外反病毒厂商成型产品（贴牌），或选择在自身现有产品拟上嵌入第三方反病毒引擎的方法，也有的厂商产品线较长，采用 OEM+自身产品嵌入引擎，两条路并举的方式大力扩张产品线。

如下表所列：

| 国内代表性信息安全厂商 | OEM 合作伙伴 | 引擎合作伙伴 |
|-------------|----------------|---------------------|
| 天融信 | Fortinet (飞塔) | Kaspersky (卡巴斯基) |
| 启明星辰 | | Antiy Labs (安天) |
| 联想网御 | Fortinet (飞塔)、 | |
| 网御神州 | Fortinet (飞塔) | |
| 方正 | | Panda (熊猫) |
| 中兴通信 | Fortinet (飞塔) | |
| 华赛 | | Symantec (赛门铁克) |
| 东方华盾 | | Kaspersky (卡巴斯基) |
| 深信服 | | F-Prot |
| 网新易尚 | Fortinet (飞塔) | |
| 交大捷普 | Fortinet (飞塔) | |
| 金山卓尔 | | Sophos、kingsoff(金山) |

由统计可以看出，基本上第一阵营、第二阵营传统信息安全厂商中的一半以上 OEM 飞塔的防毒墙，而采用嵌入引擎的方式则种类繁多，包括国外的卡巴斯基、赛门铁克、Sophos、F-Prot 以及国内的金山、安天等在内，而三线厂商则更有采用廉价但粗糙的开源的反病毒引擎 ClamAV 的解决方案。

诚然，媒体乃至业界、第三方调研机构对于此类安全产品的推崇有其自身的考虑，但无论何种安全产品形态，最终必须要满足至少两个方面的诉求：一方面使最终客户的安全运维

成本进一步下降、投资回报率提升，这是源自于最终客户的安全诉求；另一方面，对于厂商而言，其无形声誉、营销利润等需要稳步上升，走入良性发展道路，这是源自厂商对未来的发展诉求。

那么，是否在一片“歌舞升平”中，上述诉求就得以满足呢？

本文将从三个方面来分析防火墙、UTM 产品中嵌入第三方反病毒引擎的利弊之处：

1. 嵌入第三方反病毒引擎的不足之处
2. 新型防火墙、UTM 产品的设计及服务流程缺陷
3. 硬件架构的喜忧参半

第一， 嵌入第三方反病毒引擎的不足之处

首先，从反病毒引擎自身来看，其自身一定存在安全漏洞，从来自 Securityfocus 安全组织的不完全统计来看，其漏洞主要类别包括但不限于以下所列：











- l 反病毒引擎在处理特殊文件格式（如：畸形 ZIP、ARJ、CHM 等）时被欺骗；
- l 基于代理方式的反病毒引擎（如：FTP 代理、SMTP 代理等）可被精心绕过；
- l 反病毒引擎在处理特殊报头时（如：MIME、PE 等）被拒绝服务攻击 DoS；
- l 反病毒引擎自身存在缓冲区溢出漏洞（如：Sophos 中的 veex.dll 等）。

那么，引擎自身存在漏洞，对于反病毒厂商而言，其响应、修复往往需要一个周期，短则数日，长则以月来计算；而对于嵌入第三方反病毒引擎的安全产品，其修复补丁的发布与安装势必滞后一段时间；尤其是对于部署在生产环境中的安全设备而言，其所遵循的配置管理、变更管理策略更对升级需要进行多次审核。

因此，对 OEM 其他产品或者嵌入第三方反病毒引擎自身漏洞的响应不力、无法及时修复，将为该客户以及厂商本身带来一定的风险。

以下为反病毒引擎部分安全漏洞附表：

| | |
|---------------|---|
| Fortinet (飞塔) | Fortinet FortGate 绕过 CRLF 字符串 URL 过滤漏洞 2008-01-15 http://www.securityfocus.com/bid/27276 |
| | Fortinet FortGate 绕过 URL 过滤漏洞 2008-01-04 http://www.securityfocus.com/bid/16599 |
| | Fortinet FortGate 绕过 FTP 代理反病毒引擎漏洞 2006-06-21 http://www.securityfocus.com/bid/18570 |
| | Fortinet FortGate 绕过反病毒引擎漏洞 2006-03-02 http://www.securityfocus.com/bid/16597 |
| | 反病毒引擎魔法字节检测欺骗漏洞 2005-10-25 |

| | |
|------------------|---|
| | http://www.securityfocus.com/bid/15189  构造畸形压缩包欺骗漏洞 2005-10-08 http://www.securityfocus.com/bid/15046  |
| Kaspersky (卡巴斯基) | 卡巴斯基反病毒引擎 CHM 文件解析远程缓冲区溢出漏洞 2005-10-10 多个卡巴斯基产品中的 kl1.sys 文件本地栈缓冲区溢出漏洞 2008-06-04 http://www.securityfocus.com/bid/29544  卡巴斯基反病毒引擎 ARJ 格式远程堆溢出漏洞 2007-04-09 http://www.securityfocus.com/bid/23346  卡巴斯基反病毒扫描引擎 PE 文件拒绝服务漏洞 2007-01-08 http://www.securityfocus.com/bid/21901  |
| Sophos | Spophos MIME 附件拒绝服务漏洞 2008-07-10 http://www.securityfocus.com/bid/30110  Sophos CAB、LZH、RAR 文件扫描欺骗漏洞 2007-09-06 http://www.securityfocus.com/bid/25574  Sophos 多个拒绝服务与内存消耗漏洞 2007-07-27 http://www.securityfocus.com/bid/20816  恶意构造畸形 ZIP 文件扫描欺骗漏洞 2007-02-20 http://www.securityfocus.com/bid/12793  Sophos 反病毒引擎中 Veex.dll 存在多个缓冲区溢出漏洞 2006-12-15 http://www.securityfocus.com/bid/21563  Sophos 库 Visio 扫描远程堆溢出漏洞 2005-07-25 http://www.securityfocus.com/bid/14362  |

这实际上给所谓的信息安全国产化带来了非常微妙的影响,试想如果在国家保密部门所采用的国货,只是一个国产品牌,而里面的技术内核,有关厂商并不掌握。就算只是在自有防火墙/UTM 嵌入国外反病毒引擎,也等于引入了一个安全未知量。

其次,从反病毒引擎的应用环境来看,传统反病毒引擎+防火墙的方法,并非是网络反病毒的有效解决方案。单机版的反病毒产品与网关反病毒产品理应有不同,单机上以文件的静态特征码匹配+动态的启发式检测为主要诉求,而在网关处,往往病毒行为不再仅仅是以传输病毒实体文件为目标;而且还伴随着病毒体远程升级自身、下达控制指令、植入新的变种等,那么仅仅依赖单纯的静态文件检测就无法识别此类恶意行为。而这一领域反而是传统防火墙、IDS 和新兴 UTM 厂商的优势。

现有的网关防病毒引擎（以“飞塔”为例）其所采用的是将静态文件匹配引擎直接移植到网关上去，并且大量样本的识别其实是采用全哈希简单检测方式，因此性能方面自然在同等硬件环境下弱于专门为网关而设计的反病毒引擎。此外，这一方式大多仅支持少数几种可还原协议的检测，如：HTTP、SMTP、POP3、FTP等，对于采用不可还原的UDP协议等就无法检测，而后者恰恰已经成为网络蠕虫、木马传输的重要通道之一。

最后，从反病毒引擎的查杀率、误报率来看，没有任何一种引擎是能够实现零漏报、零误报等指标的，以下是来自AV-Comparatives®的一份8月份的报告（AntiVirus® comparatie August 2008®），其中关于漏报率、误报率的评测结果如下图所示：

Number of false alarms found in our clean set (lower is better):

| | | |
|------------------------------------|-----|----------------|
| 1. McAfee ³ , Microsoft | 1 | very few FP's |
| 2. ESET | 7 | |
| 3. F-Secure | 11 | |
| 4. Symantec | 12 | few FP's |
| 5. eScan | 14 | |
| 6. AVIRA | 17 | |
| 7. Norman | 19 | |
| 8. AVG | 21 | |
| 9. BitDefender | 27 | |
| 10. Kaspersky | 28 | many FP's |
| 11. Trustport | 30 | |
| 12. VBA32 | 46 | |
| 13. Avast | 47 | |
| 14. GDATA | 62 | |
| 15. Sophos ⁴ | 117 | very many FP's |

由图可知，Sophos的误报率最高，达到了117次，Kaspersky也达到了28次，一贯稳定的Symantec也有12次误报，因此反病毒引擎自身在查杀上的缺陷也不可避免的会影响到网关产品供应商的良好声誉。

第二，新型防火墙、UTM产品的设计及服务流程缺陷

对于网关防病毒产品来说，无论是由传统的硬件防火墙衍生而来，抑或是在新的UTM框架下增加反病毒功能，都从理论上具备了统一威胁管理的能力。

从设计角度而言仍然有一些问题需要指出，部分如下：

- I 位置和策略的合理性：网关位置对抗恶意代码不是一劳永逸的，一方面恶意代码的最终目标并不是网关，而是在网关之后内网内的各类终端节点，而单纯的依赖网关防毒，则会造成“单点突破，全局沦陷”的现象出现；另一方面，恶意代码无法单独存在，势必要通过各类行为（如：扫描、攻击、窃取等）扩散其影响，而这些行为对于现有直路带基于文件代理方式静态匹配的病毒功能的防火墙以及UTM设备来说，是根本无法检测的；
- I 升级频率的差异化：传统的防火墙理论上是一个稳定的面向策略的高性能安全功能组件，通过策略的配置、变更来起到安全控制；其最坏的情况下即使不能够确保预定义的安全策略有效执行，也可以通过全部阻断方式切断网络出口连接。换句话说，即使无法对内网内的威胁作出响应，也可以使之不通过网络出口进一步扩散。对于反病毒来说，其是一个可变的面向恶意代码对象的易扩展安全功能组件，特征库的升级、程序模块的升级频率远高于防火墙类安全产品

的升级。对于 UTM 产品来说，其统一化的功能架构为新功能的扩充打下了基础，但这并不是一个简单的堆叠、加法过程，相反，当可变的组件与稳定的功能组件发生同处于一个硬件及部署位置时，就会导致每个功能都会大打折扣，而反病毒引擎的不稳定概率是最高的。

- I 运维管理的特殊性：对于 IT 管理者来说，其最根本的目标是保障业务的连续性不受破坏，那么在网络出口直连的带防病毒功能的防火墙、新型 UTM 设备如果频繁的升级、变更安全策略，势必会引入一定的风险，而致使业务的可用性受到很大的损害，那么是得不偿失的。

对于新型防火墙厂商以及 UTM 厂商来说，因其自身往往缺乏足够的针对非自主研发功能模块的支持能力，势必会将客户的需求、反馈，产品中的不足、售后的疑难问题通过一定渠道传递给合作伙伴。这种方式是非常普遍的。

然而，防病毒产品与其它安全产品的支持有所不同，其它安全产品多以策略、规则的配置、变更等为主，而防病毒产品最主要的面对恶意代码本身，恶意代码的衍生、传播又具有时间复杂度、空间复杂度、本体复杂度等特性，形成了一个三维复杂度空间：



时间上：恶意代码（如：“震荡波”、“红色代码”等）在骨干网上数小时之内就传播至全球各大主要网络以及企业网络之中；

空间上：恶意代码（如：“熊猫烧香”）传播至中国大陆数千万台终端电脑之上，其中不乏大型企业内的网络终端；

本体上：恶意代码（如：“机器狗”、“磁碟机”等）多重交叉驱动保护、加密传输，自我升级，难于被快速分析并清除。

这些都为新型防火墙及 UTM 产品提出了更为严峻的挑战：

实际的恶意代码响应能力是否能够从 OEM 合作伙伴中通过某种方式获得？支持与沟通流程最快能缩短到多久？是否能满足同时支持至少 100 个企业级客户的响应请求？……甚至当具有新特性的引擎被应用至实际产品的周期有多长？是否能与市场周期同步发展等都成为需要考虑的问题。

当然，不仅仅存在以上问题，如下述案例：

当新型防火墙、UTM 设备，采用基于代理方式进行文件匹配时检测到内网内某一网段正在通过其出口向外扩散木马下载器 Trojan-Downloader.Win32.Small.gkm 时，其能做到的就是去临时封堵该网段 IP，但事实上可能该木马下载器已经将多个可绕过终端杀毒软件的恶意代码实体文件感染至内网内上百台终端机器之上时，其如何进行追踪？如何进行定位？如何评估其对业务网络所造成的严重影响？……

那么客户求助于该安全厂商，该安全厂商又进一步寻求第三方反病毒厂商进行支持，形

成一个链式传递过程，响应周期就会随之增加；但对于问题本身而言，如何复现问题、如何短时间内处理上百台已感染终端使其不进一步扩散的困难又会进一步延长响应处理过程。

显而易见，这并非一日之功，产品自身设计的复杂性与响应流程的不确定性都会影响到整个响应过程，而对于选择国外的反病毒厂商作为合作伙伴的安全厂商来说，沟通上的困难势必会使得整个响应流程变得更加冗长，而使得恶意代码的破坏进一步升级至更大范围，从而破坏业务的完整性、保密性及可用性。

第三， 硬件架构的带来的压力：

从硬件性能上来看，目前 UTM 产品不仅限于 x86 架构， ASIC 架构、NP 架构、也八仙过海，各显神通。

但由于 x86+windows 结构是病毒的乐园，现有多数主流反病毒引擎中都包含大量 x86 汇编模块，难以向其他非 x86 体系防火墙移植也就在情理当中。

同时由于非 x86 架构的诉求就在于降低批量成本，因此还会给反病毒技术带来其他挑战，ASIC 架构研发初始投入较高，性能有显著提升，但其局限性在于其存储空间有限，这意味着当病毒匹配规则数或检测规则长度之和达到上限时，就会出现无法新增匹配规则的现象，只有通过剪裁（优化）检测规则或者升级整个产品至更高一个型号系列，但这势必带来查杀能力的不稳定以及成本上的明显增加。多核 NP 架构的优势在于报文交换能力的显著增加，但是否现有的反病毒引擎能够很好的利用这一优势，例如在 64 位 MIPS 的 16 核架构上充分发挥引擎的能力，这也不是非常容易就能实现的。这些都不是传统反病毒厂商熟悉的领域。如果过多地迁就第三方引擎的支持能力，也缩小了防火墙和 UTM 厂商自身的选择空间。

综合诸多因素，都说明，在 OEM 第三方产品和嵌入第三方反病毒引擎之外，传统网络安全厂商不能放弃自己动手，丰衣足食。

值得欣慰的是，国内一些安全企业已经开始通过提升 IPS 的能力来弥补传统反病毒引擎的不足，而反病毒厂商也在做设备化的重要尝试，2008 年 6 月 19 日，作为民族软件产业的旗帜，同时也是传统防病毒厂商中的佼佼者之一的金山软件用 1452 万元收购深圳招商卓尔（二线 UTM 厂商），成立深圳金山信息安全公司，这一合作的初衷金山是希望将其“软”（反病毒引擎、团队、技术、经验、积累）与招商卓尔之“硬”（硬件架构、设计经验、稳定性、可用性等）形成优势互补，而在传统防病毒厂商与传统安全厂商之间形成一个整合的典范。

让我们用这一事件作为对未来防病毒产品趋利避害之展望……

路，就在脚下