《计算机安全》2005 年第 1 期 总第 47 期

渐成热门的网络端点安全技术

李军　清华大学信息技术研究院

信息安全涉及的技术领域和应用范围非常广泛。从技术领域来看，广义上的信息安全不仅包括对攻击和误用的防范和处理，而且包括对事故和损坏的防止和恢复。从应用范围来看，既包括以计算为主要功能的个人计算机和服务器等，也包括以通讯为主要任务的网络设备，当然还有存储设备。

就单个计算设备的狭义安全问题而言，攻击和误用只可能从人－机和机－机接口引入，而网络特别是以太网接口是当今最普及的机－机接口，它的安全防护是实现计算设备安全的关键之一；从网络计算系统的攻击和误用等安全问题来看，作为网络端点的单个计算设备是发起对网络和网络中各类设备攻击的入口，因而也是网络安全的关键之一。因此，网络端点安全(end-point security，或主机安全 host security)技术是整个信息安全中非常重要的一环，近来随着虚拟专用网络（VPN）和无线宽带接入的逐渐普及更是受到极大的关注。

端点安全的兴起

最初部署在 PC 和服务器上的专门安全产品并不是从网络的角度来设计和实现的。那时，对局域网中主机网络连接的保护主要依赖于网络边界安全设备，即安全网关（包括内嵌在路由器中的安全功能），主机上的安全措施只有操作系统本身具备的用户登陆认证和文件读写授权等。

面向边界防御的安全网关虽然重要，但却不够完整。例如，一旦黑客攻破网关而潜入某台内部主机，便可肆无忌惮地侵犯局域网内的所有其它主机。另外，网关无法防止来自内部的误用、攻击和破坏。同时，日益提高的安全过滤和控制要求，以及不断增加的带宽需要，也给网关性能带来很大压力，容易成为瓶颈和弱点。这一切都呼唤着端点安全的出现，以配合网关安全和全局管理来部署全方位（holistic）、多层次的安全。

首先出现的专门主机安全产品是台式或服务器防病毒软件。随着病毒的主要传播介质从软盘变为网络，而其它通过网络（特别是局域网或内部网）对网络

端点的攻击和入侵成为主机安全的主要问题，端点安全开始兴起，出现了个人防火墙（personal firewall）等专门的端点安全产品。

个人 VPN 用户的增多，使网络上班族（telecommuter）和频繁出差族（road warrior）通过 IPSec VPN 客户端软件接入内网带来的安全隐患受到关注。特别是 SSL VPN 的热炒，虽然并没有带来想象中的个人 VPN 用户爆炸，却大大提高了人们对通过 VPN 接入网站或服务器的端点本身安全的前所未有的期望和要求。如果用户可以从一台主机通过 VPN 接入内网，但主机本身不安全，如已被病毒感染或另有不安全的网络连接（split tunnel）等，将对内网带来极大威胁。

无线局域网（WLAN）的迅速普及和它在较长时间内安全控制的缺乏，也大大推动了端点安全的兴起。人们终于看到了单纯关注边界安全而忽略端点安全的弊病。

今天的端点安全已经涵盖了设置管理、防病毒、防入侵和防火墙等多种功能。其中的设置管理在网络端点（直接或经由 VPN）接入内网之前通过检查主机各方面安全设置和执行状态来确保其符合内网的安全要求。检查的内容可以包括软件（特别是操作系统）版本和补丁、防病毒产品（包括引擎和病毒库）版本和运行情况、防火墙策略设置和运行情况等。端点安全控制检验产品的主要供应商有 Sygate 和最近刚被 CheckPoint 收购的 Zone Labs 等。这些产品通过与 Cisco、Juniper 等主力安全网关产品的配合，实现端点设置管理。

端点安全的发展

端点安全的产品虽由 SSL VPN 和 WLAN 催化而渐渐成为热门，但它的发展并不受限于此，而是开始成为一个相对独立的产品类别，预期将有较快市场增长。据 Yankee Group 估计，仅就企业级的远程端点安全（Remote End-Point Security，REPS）产品而言，2001 年的总产值只有 2 千万美元，而到 2006 年将增至 2 亿 6 千万美元。

在产品层面，它既可从功能角度被分为提供端点保护（end-point protection）的产品（如主机内置防火墙等）和保证端点完整（end-point integrity）的产品两类，也可以从操作的角度被分为被管理的主机（managed host）和无管理的主机（unmanaged host，如自动售货机等）两种，亦或从软件

角度被分为安装的软件（installed software）和加载的代理（loadable agent）两样等。

在技术层面，它的发展可以从下面几个方面初见端倪。

从分立到集成的端点安全

虽然最初的端点安全产品是以桌面防病毒、个人防火墙、主机防攻击、VPN客户端等单独的软件产品出现的，但随着人们开始将端点安全作为一个完整问题加以对待，特别是对设置管理要求的日益突出，端点安全正经历着一个从分立到集成的过渡。

以 Cisco 的安全代理（security agent）为例，它的目标是为网络端点提供威胁防护（threat protection）。 它在单一产品中集合并扩充了主机式防攻击、分布式防火墙、恶意代码防范、操作系统完整性保障和审计记录整合等多项端点安全功能，从而达到提高安全水平和降低运行成本的目的。

在端点安全集成软件方面市场份额较大的是由华人郭毅先生 1995 年创办的 Sygate。Sygate 的安全代理集成了针对应用的防火墙引擎和基于应用的入侵防范引擎，可以自动定期检查端点主机相对安全设置要求（包括防病毒等各种安全软件状态，病毒特征库、防火墙策略表、入侵防范特征库版本，以及注册表内容、操作系统设置等）的符合性，并将不符合的端点隔离到“ 矫正区域 ”，通过升级、更新或补丁使其达到符合性要求。

当然，从分立到集成并不只有将所有端点安全功能融合为一个厂家的一款产品。至少在不远的将来，它的表现形式更多应为以设置管理为纽带的多厂家产品的集成和互动。换一个角度说，也就是由单一主机上多个代理组成的代理组来完成端点安全。

从软件到硬件的端点安全

完全由软件实现的端点安全产品通常是运行在主机的操作系统之上的应用程序，不但大大增加了 CPU 的负担，而且完全依赖于操作系统，无法防止黑客利用其它应用软件和操作系统的漏洞获取主机控制权限，特别是难以避免主机用户因安装含有恶意代码的软件而造成的问题。

解决端点安全问题，必须有相应的硬件支持。有 200 多厂商等单位参加的可信计算组织（Trusted Computing Group, TCG）已经制定了硬件和软件的标准来增强主机安全，其中非常重要的就是用来存放密钥、密码和数字证书的微控制器，即可信平台模块（Trusted Platform Module, TPM)。与此同时，一些厂商也开始研制部署于网络接口的基于硬件的端点安全产品。这些产品以安全网卡形式出现，最终也可能集成到主版。当然，由于增加成本的原因，这类产品的应用还只多见于服务器。

在专用硬件网卡上内置的防火墙、VPN 以及入侵监测防护器（IDP）除了可以分担主机 CPU 的负担，还由于它可以独立运行而能够更好地支持中央管理，防止主机用户或通过盗用主机引入的问题，甚至在一定程度上可以阻断从被攻破的主机上发动攻击。例如，可以使网卡内置的安全功能具有单独的安全认证，使得安全策略的设置和更改只能通过独立的配置手段进行。甚至可以使配置控制权不在主机而在管理中心，因而即使黑客侵入了某个主机并获得了它的管理员权限，也不能禁用或更改网卡内置的安全功能。又如，专用硬件网卡上内置的防火墙能够自动防止该主机伪造网包 IP 地址等。

专用硬件网卡安全产品面世较早的是 3Com 开发的嵌入式防火墙。它对操作系统和最终用户透明，为高风险服务器提供防入侵、防篡改和防破坏手段。其内置安全处理器可与 Windows 操作系统配合从主机 CPU 上卸载 TCP/IP 处理、IPSec VPN 密码和认证计算、以及安全策略执行，从而提高主机系统总体性能。国内也有厂家正在开发基于 Intel 低端网络处理器的嵌入式入侵防御网卡产品。

从离散到综合的端点安全

端点安全并不是简单地把网关安全推向端点，期望由集成了所有安全功能的安全代理解决所有问题。端点安全要与网关安全和其它安全设施密切配合，分工协作，才有可能构架全面完整的安全防护保障体系。例如，IDP 的负担可以通过用户配置由网关和端点协调承担，由网关的网络入侵检测防护（NIDP）对 4 层及以下协议攻击特征的监控，而由端点的主机入侵检测防护（HIDP）承担对于应用层（4 层以上）协议攻击特征的监控，特别是与端点防火墙结合，针对端点实际运行的应用实施有的放矢的防护。

端点安全的重要组成部分是设置管理或面向符合性的检查、隔离和矫正。要做到这一点，端点安全早已走出离散的、完全独立运行于单个主机的模式，而是正在与中央管理产品综合在一起，逐步形成完善的全方位、多层次安全体系。中央管理产品本身也可以是分层分布的，其中有些功能可以集成在网关上。这样的布局使得安全解决方案更加严密，也具较好的灵活性。当网络的状况变化时，管理中心可以根据实际情况调整对于各个端点的安全要求和安全策略部署，并通过给各个端点分发任务和监督实施来保证整个网络系统的安全性。

网络设备的主力厂商近来都争先恐后地增加了对端点安全的支持。Cisco 在路由和交换产品上实现的网络接受控制（Network Admission Control，NAC）技术可以与 IBM 的 Tivoli 网络和系统管理客户端软件配合，在用户或设备接入网络时检查其符合性，并可实现隔离并提请矫正。Juniper 的端点防卫计划(Endpoint Defense Initiative)解决方案，使 NetScreen Secure Access SSL VPN 设备与多种优秀端点安全产品达成强大的整合能力，合作伙伴包括 InfoExpress、McAfee、Sygate、Symantec、TrendMicro 和 WholeSecurity 等公司。

端点安全的未来

端点安全涵盖的决不只是主机。任何一个设备接入网络时都可被视作一个网络端点，而它既可以是主机，也可以接纳更多端点而成为一个网关。

端点安全的发展很快，并呈现出整合的态势。一方面，企业通过并购或结盟将产品整合成解决方案，如 CheckPoint 就通过收购端点安全顶尖企业 Zone Labs 获得完整的产品组合，提出全接入保护（Total Access Protection，TAP），并把防间谍（或间谍软件 spyware）引入集成的端点安全。另一方面，端点安全标准化的努力也在快马加鞭。例如，在对端点接入网络实施安全策略强制时，目前还是有很多案例因为成本考虑而使用基于 DHCP 的方案，即给不满足符合性的端点分配专门安排的 IP 地址，以对这类端点的行为加以限制。有经验的用户或黑客很容易躲避这种限制。更为严谨的方式有基于 802.1x 的方案，也有基于网关的方案，但需要标准化工作以满足互操作要求。

2004 年 5 月，可信计算组织 TCG 成立了可信网络连接（Trusted Network

Connect, TNC）分组（TNC Sub Group, TNC-SG)。作为 TCG 中基础设施工作组（Infrastructure Work Group）的一部分，它将 TCG 的视野延展到了网络的安全性和完整性，设计防止不安全设备接入和破坏网络的机制。一些重要网络和安全公司如 Foundry、 Extreme、Funk Software、InfoExpress、iPass、Juniper、Meetinghouse Data Communications、Trend Micro、Network Associates、Sygate、Symantec 和 Zone Labs 等参加了 TNC。

TNC 可以在端点安全技术和产品的发展中发挥重要作用。它将为可互操作的安全方案制定实施安全策略强制以防止不安全系统或设备接入网络的规范。这些规范将利用现存工业标准，并在需要时起草和提议新的标准。这些标准将包含端点安全构件之间、端点主机或网络设备之间的软件界面和通信协议。它们将通过认证和符合性检查保障端点的完整性，对不满足要求的端点提供隔离并尽可能加以矫正。

参考文献：

Matthew Kovar, Enterprise Remote End-Point Security Products: Driving Security Policies to the Last Mile, Yankee Group

Michael Rasmussen，Demand for Endpoint Security Growing，Forrester Research

李军，“ 第三代安全网关：中国安全产业新机遇 ”，互联网周刊，总第 253 期，第 43 期，2003 年

李军，“ 防火墙上台阶：安全网关多层过滤技术的走向 ”，《信息网络安全》，总第 43 期，第 7 期，2004 年