入侵防御系统IPS，技术成熟了吗？ PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/166/2021_2022__E5_85_A5_E4_BE_B5_E9_98_B2_E5_c101_166590.htm IPS（入侵防御系统）提出了多年，一直有个声音认为IPS会取代IDS（入侵检测系统），但是几年过去了，情况并非如此，那么IPS 目前到底处于什么状态呢？ 据调查，目前59%的用户部署了IDS，27%的用户将IDS列入购买计划，62% 用户在关注 IPS，并且7%的用户有意向购买 IPS，这些数据表明，IDS和IPS 在国内都呈现出繁荣发展的前景。 这与几年前一些研究机构预计的“ IPS将逐步取代IDS ”的看法截然不同。IPS 既没有得到“ 一览众山小 ”的市场局面，IDS 也没有“ 节节败退 ”，是什么原因使得人们的预测出现了如此大的偏差呢？要想找出其中的原因，不得不从研究历史出发，看看IDS 和IPS 都是如何发展的。需求决定IDS 不会消沉 安全防护是一个多层次的保护机制，它既包括企业的安全策略，又包括防火墙、防病毒、入侵检测等产品技术解决方案。而且，为了保障网络安全，还必须建立一套完整的安全防护体系，进行多层次、多手段的检测和防护。IDS正是构建安全防护体系不可缺少的一环。 虽然有很多用户对IDS 是否具有存在价值表示过质疑，但到目前为止，更多的用户是在关注如何最大程度地发挥IDS 的作用，来保障网络的安全。 据市场统计显示，2005 年 IDS 可以占到安全市场全年总额的11.2%，市场销售额达到5. 5亿元。而2004 年国内IDS产品全年销售额是3.8亿元，占中国网络安全市场全年市场份额的 10.9%。2003 年IDS的市场销售额是2.75亿元。可以看出，随着国内用户的成熟，IDS在网络安

全市场中也是处在一个稳定的发展阶段。在这种情况下，谁能说IDS的市场会江山不再呢？ 促使IDS 得到广泛应用的另一个因素是，Slammer、冲击波等针对系统漏洞的攻击不断增多，新的软件漏洞不断被发现，一些分析系统缺陷、编写攻击程序或制作蠕虫病毒的简单工具也在不断发展之中，从发现缺陷到释放出蠕虫病毒的时间间隔也在进一步缩短，用户需要一种可以检测攻击的有效工具，IDS 就是其中的一种。 自身改进打破IDS 灭亡论 虽然前一时间IPS取代IDS 的呼声日渐高涨，而且Gartner 发表的“ IDS将死 ”言论更是让这两种技术的争斗达到了白热化，但在国内，IDS还没有受到“ 灭亡论 ”的太大影响，这主要是因为IDS不断地进行着改造。目前的IDS 技术是需要有比较大的改进才能满足客户的需要，可能需要细分市场做出不同的产品来满足不同的客户。 从安全厂商来看，安氏中国、绿盟科技、McAfee、天融信、方正、冠群金辰、联想、东软、中科网威、启明星辰等众多厂商都有多款百兆和千兆的 IDS 产品。从对这些主流IDS 产品的评测来看，IDS 产品在性能方面也是不断进步的。比如， 2002 年2003 年的百兆IDS 产品，在64 字节100%压力下平均检测能力仅有40.2%，而2003 年2004年，部分百兆IDS 产品检测能力已达到100%，这标志着百兆IDS 产品在性能方面已经成熟。而千兆IDS 产品的性能也有了长足的发展，捕获数据包的能力每秒67 万85 万，最高可达140 多万，对大流量网络的适应能力明显增强。还有在功能方面，部分IDS 产品几年前就具备了网络流量分析、页面重组、内容恢复、事件回放等功能，如今不仅功能更为完善多样，而且功能的模块化也更有利于用户根据实际需要进行定制和应用。 近年来，IDS在网络

中的应用逐渐增多起来。在很多对安全等级要求很高的证券、金融以及电信的网络中，我们都能发现IDS的身影。某证券公司的IT主管谈到：“ 随着企业网络结构的不断扩大和日益复杂，由内部员工违规引起的安全问题变得突出起来，防火墙、防病毒等常规的安全手段只能对付外部入侵，对于内部违规行为却无能为力。而IDS 可以审计跟踪内部违反安全策略的行为。另外，IDS 可以记录、报警各种安全事件，有利于进行安全审计和事后追踪，对于追溯和阻止拒绝服务攻击能够提供有价值的线索。 ”IDS 缺陷成就IPS 不过我们同时也看到，也有很多用户反应IDS 带来的麻烦大于贡献。有用户反映，IDS 的误报率太高，只要一开机，警报便响个不停，在每天发出的上万条的报警信息中，真正有价值的信息却寥寥无几，而从上万条信息中挖掘出有用信息费时又费力，通常需要设立专人负责管理IDS，这在缺乏IT人才的企业中是很不现实的。 想要解决误报和漏报的问题，要综合运用多种检测机制，包括特征对比、协议异常分析等技术，同时需要引入数据挖掘技术、神经网络、专家分析系统等技术以提高信息分析能力。 未来的IDS还需要面向宽带高速实时的网络环境，引入数据挖掘、分布式部署、免疫和神经网络技术，并且适应 IPv6 的技术要求。 很多用户希望IDS 能够增加主动阻断攻击的能力，在危害出现时能够直接将其阻断。用户的这种希望并不是空穴来风，而是与当前的安全形势息息相关。系统漏洞屡屡被攻击，主动防御和应用安全的压力从来没有如此凸显过。一方面系统的复杂性在不断提高，几乎每周都会有系统缺陷被发现；另一方面利用高危缺陷进行入侵和传播的攻击技术也在快速发展，用户需要一种能够实时阻断攻

击的安全技术。 从工作原理上来看， IDS技术属于被动式的反应式技术，这种技术在安全威胁传播速度较慢时并没有显现出太大问题，随着威胁传播速度的加快，留给人们响应的时间越来越短，使用户来不及对入侵做出响应，于是喊着主动防御口号的IPS得到了一定的市场机会。 IPS 靠主动防御抢占市场 混合威胁不断发展，单一的防护措施已经无能为力，企业需要对网络进行多层、深层的防护来有效保证其网络安全。真正的深层防护体系不仅能够发现恶意代码，而且还能够主动地阻止恶意代码的攻击。在当前混合威胁盛行的时代，只有深层防护才可以确保网络的安全。而IPS(入侵防护系统)则是提供深层防护体系的保障。 IPS的出现可谓是企业网络安全的革命性创新。 从技术的同源性上来看， IPS 和IDS之间有着千丝万缕的必然联系，IPS 可以被视作是增加了主动阻断功能的IDS。例如 McAfee 的IntruShield 以在线方式接入网络时就是一台IPS，而以旁路方式接入网络时就是一台IDS。但是，IPS 绝不仅仅是增加了主动阻断的功能，而是在性能和数据包的分析能力方面都比IDS 有了质的提升。 由于增加了主动阻断能力，检测准确程度的高低对于IPS来说十分关键。IPS厂商综合使用多种检测机制来提高IPS的检测准确性。据Juniper 的工程师介绍，Juniper 在IDP（Juniper 将自己的入侵防护产品命名为IDP) 中使用包括状态签名、协议异常、后门检测、流量异常、网络蜜罐、哄骗检测、第二层攻击检测、同步泛洪检测、混合式攻击检测在内的“ 多重检测技术 ”，以提高检测和阻断的准确程度。Juniper还在不断增加IDP能够解析的协议数量，最近将支持50 种协议增加到60多种，不断为防止新型攻击开发新的检测方法。 除了检测机制外

，IPS 的检测准确率还依赖于应用环境。一些流量对于某些用户来说可能是恶意的，而对于另外的用户来说就是正常流量，这就需要IPS 能够针对用户的特定需求提供灵活而容易使用的策略调优手段，以提高检测准确率。 McAfee、Juniper、ISS同时都在 IPS 中提供了调优机制，使IPS 通过自学习提高检测的准确性。 引入弱点分析技术是IPS的另一个亮点。IPS厂商通过分析系统漏洞、收集和分析攻击代码或蠕虫代码、描述攻击特征或缺陷特征，使IPS 能够主动保护脆弱系统。由于软件漏洞是不法分子的主要攻击目标，所以几乎所有IPS厂商都在加强系统脆弱性的研究。ISS、赛门铁克分别设立了漏洞分析机构。McAfee 也于日前收购了从事漏洞研究的 Foundstone 公司，致力于把漏洞分析技术与入侵防护技术结合起来，使关键资源得到主动防护。Juniper设有一个专门的安全小组，密切关注新的系统弱点和蠕虫，每周都会发布攻击签名和基于严重等级的紧急签名更新， Juniper 提供的攻击签名是基于弱点和安全漏洞，而不仅仅是黑客已经使用并且造成破坏的安全弱点。 McAfee 公司北亚区技术总监陈联认为，目前严重的安全事件大多数是由缓冲区溢出所导致，所以McAfee 在自己的实验里加强了对溢出型漏洞的研究和跟踪，并且把针对溢出型攻击的相应防范手段推送到IPS 设备的策略库中。这项缓冲区溢出分析技术使得McAfee的IPS设备能够检测七层的数据包，实现对应用的主动保护。 赛门铁克在IPS设备中采用了漏洞阻截技术。通过研究漏洞特征，将其加入到漏洞签名库中，IPS 就可以发现符合漏洞特征的所有攻击流量。冲击波及其变种都利用了RPC（微软操作系统的一个漏洞）漏洞。赛门铁克通过研究并提取RPC 漏洞的特征，组成特征签名

并将其推送给 IPS 设备。在公布漏洞和病毒爆发的一段间隔里，用户只需将漏洞特征签名自动下载，就可以在冲击波及其变种大规模爆发时，直接将其阻断，从而赢得打补丁的关键时间。 主动防御是安全根本 绝大多数IDS 系统都是被动的，而不是主动性的。在攻击实际发生之前，IDS 往往无法预先发出警报。IPS则倾向于提供主动性的防护，其设计旨在预先对入侵活动和攻击性网络流量进行拦截，避免其造成任何损失，而不是简单地在恶意流量传送时或传送后才发出警报。IPS是通过直接嵌入到网络流量中而实现这一功能的，即通过一个网络端口接收来自外部系统的流量，经过检查确认其中不包含异常活动或可疑内容后，再通过另外一个端口将它传送到内部系统中。这样一来，有问题的数据包，以及所有来自同一数据流的后续数据包，都能够在IPS设备中被清除掉。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com