IPSvsIDS势不两立还是相辅相成？ 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_IPSvsIDS_E5_8A_c101_166579.htm 2003年8月，Gartner公司副总裁Richard Stiennon发表的一份名为《入侵检测已寿终正寝，入侵防御将万古长青》的报告，提出入侵检测系统Intrusion Detection System（IDS）已经难以适应客户的需要。IDS不能提供附加层面的安全，相反增加了企业安全操作的复杂性。入侵检测系统朝入侵防御系统Intrusion Prevention System（IPS）方向发展已成必然。 一石激起千层浪。刚刚从IDS脱颖而出的IPS，一时间竟然成了IDS的天敌。两年多来，尽管事实上IDS非但没有退出安全产品阵列，反而不断更新、依然占领着继防火墙之后第二大的安全产品市场份额，但是IDS行将就木的宣传不仅引发了信息安全体系建设上的争执与混乱，而且给客户的信息安全产品选型造成了不应有的压力与彷徨。1. IDS的功能与缺陷 IDS本质上是一种监听系统，它依照一定的安全策略，对网络与系统的运行状况进行监测，尽可能发现、报告、记录各种攻击企图、攻击行为或者攻击结果，以保证信息系统的机密性、完整性和可用性。IDS可分为主机型HIDS和网络型NIDS，目前主流IDS产品均采用两者有机结合的混合型架构。1.1 IDS的传统优势 NIDS使用原始网络信息作为数据源，利用运行在随机模式下的网络适配器实时监听和分析通过网络的所有通信，收集相关信息并记入日志；而HIDS则通常安装在被检测的主机之上，与该主机的网络实时连接，负责对系统审计日志进行智能分析和判断。若发现非法入侵或者违反统计规律的行为异常，IDS会立即发出警报，由系统管

理员进行决策处理。IDS的传统优势在于：整体部署，实时检测，可根据用户的历史行为模型、存储在计算机中的专家知识以及神经网络模型，对用户当前的操作进行判断，及时发现入侵事件；对于入侵与异常不必做出阻断通信的决定，能够从容提供大量的网络活动数据，有利于在事后入侵分析中评估系统关键资源和数据文件的完整性；独立于所检测的网络，黑客难于消除入侵证据，便于入侵追踪与网络犯罪取证；同一网段或者一台主机上一般只需部署一个监测点就近监测，速度快，拥有成本低。1.2 IDS的明显缺陷 IDS最明显的缺陷有：被动防御的监听方式限制阻断。目前IDS只能靠发阻断数据包来阻断建立在TCP基础上的攻击，对于建立在UDP基础之上的入侵则无能为力；基于特征的入侵检测技术落伍。由于缺少信息管理，难于抵挡Canvas和MetaSploit等欺骗工具的攻击和渗透；误报与漏报率高于客户预期。有些IDS产品每天会产生大量的异常报告，其中绝大多数属于非攻击行为，需要具有相当专业水准的网络安全管理员进行甄别，有时甚至会给客户造成难于忍受的负担；对于检测主机的依赖性。由于HIDS安装于检测主机之上，不仅消耗检测对象的部分资源，影响到被检测主机的效率，而且还必对不同的主机及其系统环境设计和安装各自的HIDS。2. IPS的优势与弱点 提到IPS，人们常常会谈到一个公式: IPS = Firewall IDS；也有文献认为，将IDS的传感器置于网络通信线路之内（In-line），让所有网络通信量必须通过它，就得到了一台IPS。这两种看法均有偏颇之处，但是却殊途同归地道出了一个事实：IPS来自IDS。2.1 IPS的原理与分类 青出于蓝而胜于蓝。IPS串联于通信线路之内，是既具有IDS的检测功能，

又能够实时中止网络入侵行为的新型安全技术设备。IPS由检测和防御两大系统组成，具备从网络到主机的防御措施与预先设定的响应设置。图1是北京基格网络技术有限公司研制的基格领袖IPS原理框图，在同类产品中颇具代表性。图1. 入侵防御系统IPS的原理框图 目前，从保护对象上可将IPS分为三类：基于主机的入侵防护（HIPS），用于保护服务器和主机系统不受不法分子的攻击和误操作的破坏；基于网络的入侵防护（NIPS），通过检测流经的网络流量，提供对网络体系的安全保护，一旦辨识出入侵行为，NIPS就阻断该网络会话；应用入侵防护（AIP），是将基于主机的入侵防护扩展成为位于应用服务器之前的网络信息安全设备。2.2 IPS不可低估的优势 实时检测与主动防御是IPS最为核心的设计理念，也是其区别于防火墙和IDS的立足之本。为实现这一理念，IPS在如下四个方面实现了技术突破，形成了不可低估的优势：在线安装(In-Line)。IPS保留IDS实时检测的技术与功能，但是却采用了防火墙式的在线安装，即直接嵌入到网络流量中，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；实时阻断（Real-time Interdiction）。IPS具有强有力的实时阻断功能，能够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；先进的检测技术（Advanced Detection Technology）。主要是并行处理检测和协议重组分析。所谓并行处理检测是指所有流经IPS的数据包，都采用并行处理方式进行过滤器匹配，实现在一个时钟周期内，遍历所有数据包过滤器；而协议重组分析是指所有流经IPS的数据包，必须首先经过硬件级预处理，完成数据

包的重组，确定其具体应用协议。然后，根据不同应用协议的特征与攻击方式，IPS对于重组后的包进行筛选，将可疑者送入专门的特征库进行比对，从而提高检测的质量和效率；特殊规则植入功能（Build-in Special Rule）。IPS允许植入特殊规则以阻止恶意代码。IPS能够辅助实施可接收应用策略(AUP)，如禁止使用对等的文件共享应用和占有大量带宽的免费互联网电话服务工具等；自学习与自适应能力（Self-study &amp. Self-adaptation Ability）。为了应对黑客们处心积虑、花样翻新的攻击手段，IPS必须具有人工智能的自学习与自适应能力。能够根据所在网络的通信环境和被入侵状况，分析和抽取新的攻击特征以更新特征库，自动总结经验，定制新的安全防御策略。2.3 IPS不可忽视的弱点 有其利必有其弊。IPS的主动防御优势也决定了它的下列弱点：总体拥有成本（TOC）高。浩大的高可用性（HA）实时计算需求决定了IPS必须选用高端的专用计算设备，但是可观的总体拥有成本却使不少用户望而却步；单点故障（Single-point Fault）。IPS的阻断能力决定其必须采用网络嵌入模式，而这就可能造成单点故障；性能瓶颈（Performance Bottle-neck）。即使IPS设备不出现故障，它仍然是一个潜在的网络瓶颈，不仅会增加滞后时间，而且会降低网络的效率，因此，绝大多数高端IPS产品供应商都通过使用自定义硬件（FPGA、网络处理器或者ASIC芯片）来提高IPS的运行效率，以减少其对于业务网络的负面影响；误报（False positive）与漏报（False negatives）后果同样严重。在网络流量几乎成几何级数增加的情况下，一旦生成警报，最基本的要求就是不让“ 误报 ”有可乘之机，导致合法流量也很有可能被意外拦截。如果触发

了误报警报的流量恰好是来自上级、合作伙伴和客户的重要信息，IPS不仅实施了一次性错误阻断，而且会切断与他们的信息通道，其结果不言而喻。3. IPS目前不可能取代IDS 我们既要看到IPS蓬蓬勃勃的增长势头，又要承认IDS在入侵检测领域的传统优势，肯定IPS目前尚不可能完全取代IDS的基本事实，在建立自己的网络与信息安全体系的过程中，将两者有机地结合起来。3.1 IPS增长势头强劲 根据IDC发布的案例，美国的一家财务公司，在全球有12个分支机构，原计划使用多台防火墙并搭配250个许可证的IDS。最终，该公司仅用了30个许可证的IPS产品就实现了全球网络的入侵防御，而管理人员只需要3至4人，效率却提高了6倍以上。 波士顿Sappi Fine报社信息安全总监Jim Cupps说，作为具有10,000桌面设备和数百台基于微软服务器的公司，现在开始使用Determina基于主机的IPS，称之为内存防火墙的专用服务器，主要作为防御蠕虫的附加件。基于行为的内存防火墙能够监测缓冲区溢出攻击，"它并不能替代打补丁，但是它让我们不必立即打补丁，我们战胜了补丁恐慌’，如果漏洞确实存在，入侵防御系统能够帮忙。"图2. IPS市场销售统计与预测（2003-2008） 在受益于IPS的优势和效益的同时，不少用户对于其弱点和不足，也能给与理解与宽容。大名鼎鼎的网络安区专家Mathias Thurman在IDC的《计算机世界》上写道，由于In-line安装，IPS设备的故障可能根本上阻断网络通信。因此，我们需要选择具有容错能力的IPS，即故障时能让通信畅通。我愿意承担短时期自我开放的风险，也不愿面临数以千计的雇员无法工作，损失收入和劳动生产率的局面。 正是由于IPS主动防御和易于管理的特性，致使其销售也正在突飞猛进。图2是来自

于IDC的2003-2008年IPS销售额的统计与预测。从此图中可以看到，到2008年，IPS的销售额可高达11.8亿美元，比2005年增加将近一倍。 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