企业入侵检测系统：破解IPS迷雾 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__E4_BC_81_E4_B8_9A_E5_85_A5_E4_c101_166582.htm 2005年秋，由全球多家系统软件公司进行的一项联合调查表明，超过66%的企业用户认为，“ 系统渗透 ”将会成为威胁企业IT安全的首要元凶。调查同时披露了目前发生最多的八项信息安全威胁，包括了：病毒、系统渗透、拒绝服务、内网滥用、欺骗、由于离职人员造成的数据或网络损失、非授权的内部访问。 虽然86%的被调查者使用了防火墙，但大多数情况下这些防火墙无法有效反击入侵行为。因为常见的防火墙主要是用来防御直接的可疑流量比如在安全策略没有授权的情况下，拒绝访问者telnet到一台保护设备上，或者允许某些数据流通过如Web服务器通信。 目前的问题是，安全模型在变化: 在越来越多可以穿越防火墙的流量中，夹带着攻击，即面向应用的攻击。大部分防火墙检查的层次主要集中在传输层以下，即使是优秀的防火墙也只能提供一小部分深度检测能力。 当企业服务器接受了这些“ 糖衣炮弹 ”后，攻击者就可以此为跳板，向企业内网发送大量的攻击性报文。一旦这些人在服务器上留下“ rootkit ”、“ back door ”等后门，那么它就可以在任何时间、任何地点无限制的访问企业整个信息系统。 更要命的是，几乎所有的企业都有过从内部遭受攻击的经历，虽然很多情况下这些“ 内贼 ”自己都不知道，毕竟像VPN、无线网络、笔记本电脑，都可以穿过防火墙访问互联网。 当然，有用户使用IDS来监视系统安全，并希望通过与防火墙联动来防范入侵。不过前提是，只有当入侵者使用2800bps的网络

速度入侵企业网络的时候，IDS才有足够的反应时间来调度其他安全设施配合！缓慢的时间戳根本无法阻止类似“ Slammer ”、“ Blaster ”等高速繁殖带来的灾难。 为了解决以上问题，采用实时在线方式的企业入侵检测系统（IPS）被投入使用。IPS的初衷是针对企业应用进行防御，由于所有流量都要从IPS中通过，保证了设备采取防御的时间。不过带来的问题是，深入包检测让人对于设备的性能有所担忧，特别是当防护选项全都开启的时候，而且IPS一旦出现误报，直接后果肯定比IDS大。 正是由于心存疑虑，导致众多国内用户对IPS迟迟不敢下手。为此，我们联合了国内外众多IPS厂商，同时结合评测实验室的报告，组织了此次IPS的技术专题，主要从国内用户关心的方面入手，为读者呈现一幅清晰的IPS应用脉络。 破解一 诠释IPS“ 性能 ”说到性能，目前为止还没有一个简单的量化指标。从国内外大量第三方评测机构的报告分析，吞吐率与延时可以作为简单的参数。但业内人士认为，这必须结合用户的具体需要来看，否则很难讲其意义有多大。因为不同厂家IPS支持的协议数量、默认功能开启程度、检测精细度、承受攻击的时间等指标差异极大，获取性能指标的前提条件有很大不同，如果单独依据厂家提供的DataSheet，对于用户的选择是很难有帮助的。 根据经验，业内众多Hi-End级IPS厂家（笔者借用了音响发烧友的术语），其产品都要支持：HTTP、DNS、FTP、DoS、ICMP、RPC、SSH、Mail、Telnet、Backdoors、Finger、False negatives、Database、Reconnaissance等攻击方式以及企业四大协议（HTTP、FTP、SMTP、POP3）以外的新应用，如MSN等。 国内用户还必须了解，IPS的性能评估数据不能是在“ 裸奔 ”或仅打开少量

过滤器的前提下取得的，也不能是单纯的测试流量，如单纯的UDP流量或单一的包长度。用户应当结合自身情况判断: 如企业部署了VoIP的应用，那就必须去评价它的时延抖动问题，而且要在语音数据流中混杂一般数据模拟实际情况。 有条件的用户，也可以查阅第三方报告，分析IPS在负载情况下的效能参数，像对随机端口发送的UDP流量、考虑和不考虑处理延时情况下的HTTP最大压力流量等。（《网络世界》报社稍候将会为读者奉上国内最权威的IPS横向评测报告） 目前，一些国内用户已经开始选购前的自行测试。以北京大学与TippingPoint的合作为例，该校信息中心正在结合校内的流量情况进行实地检测。据悉，当前北大校园网骨干流量为800Mbps，而且其中的混合协议流庞大，对于类似应用，通常的做法是采用校内真实流量预测或者用“ 72%的HTTP 20%的FTP 4%的UDP ”流量模型评估。 也有专家指出，国内用户不要过度迷信数值，而要分清自身应用的特征。因为很多Hi-End级IPS厂家，可以提供在64/256/350/440/540/1514字节（根据应用与压力不同）条件下，实现250/500/750/1Gbps的线性吞吐与极低延时。但如果用户只有一个100Mbps骨干带宽出口，且近期不会升级网络带宽，就没必要刻意要求1Gbps数据传输时的性能指标。 高性能自然是好事，但这多伴随着高成本。特别是大部分用户在日常应用中，遇到如此五花八门数据包的情况极为少见，普通情况是：对于纯HTTP协议，一般每秒最多100条TCP连接、每秒25位新用户，平均包长1000字节，每秒最多110000个包；对于混合协议，一般是540字节HTTP与256字节UDP，每秒最多550条TCP连接，平均包长900字节，每秒最多130000个包，最多11000条开放连接。

另外，关于IPS自身设计与性能的关系，在此也有必要澄清一下。目前IPS设计主要分为FPGA（现场可编程门阵列）与X86（CPU加交换板）两种架构（包含NP）。其实这两种架构并非彼此独立，在一些Hi-End级IPS产品中，这些芯片都是存在的。 TippingPoint网络技术顾问李臻认为，从芯片本身分析，FPGA这种封装方式具有灵活、可编程的优势，而McAfee安全顾问陈纲更直接称其为一种廉价高效的专业芯片。一些大厂用其对进入数据包进行特征匹配，在这种工作上，FPGA区别于传统X86架构的顺序工作方式，性能是有很大提升的。不过Juniper大中华区新兴技术经理吴若松表示，并非所有采用FPGA的IPS产品，性能都会优于使用X86架构的产品，或者说用户应该关注，满足充分的安全防御前提下的性能可用。这就像音响发烧界的一个经典案例：普通立体声音箱采用左右两分频技术，但很多Hi-End级音箱为了获得更加纯净的声音表现，往往会采用多分频技术（三、四分频），但有些Hi-End级厂家，如丹拿音箱，由于自身的设计特点和结构的特殊性，只需要进行两分频就可以获得比其他厂家更加优秀的声音。 所以说，采用FPGA可以带来性能优势，但前提是自身的设计适合FPGA架构；同理，一些采用X86架构的Hi-End级IPS厂家，只要是自身设计独到，同样可以获得优秀的性能。Juniper大中华区新兴技术经理吴若松认为，用户对于产品架构差异与性能之间的关系，确实不用过于敏感，从目前市场情况看，只要是负责任的厂家的产品，都可以满足要求。 破解二 细看“ 误报与漏报 ”对于“ 误报 ”、“ 漏报 ”的问题，用户的看法是，由于IPS会对攻击采取行动，因此误报带来的灾难显然要比IDS产品大。不过TippingPoint中国

区业务总监贾泉海表示，各大IPS厂商研发的主要精力都在于此，产品的检测精度在2年内已经有了质的提升。 目前，在Hi-End级IPS厂家中流行的检测技术有两个方向：一种是TippingPoint提出的并行处理检测；另一种是McAfee提出的协议重组分析（Radware、Juniper、ISS等主流厂家皆有类似技术）。 所谓并行处理检测是指，所有流经IPS的数据包，都要被送入FPGA单元中进行过滤器（逻辑门）匹配。由于常用的过滤器超过2000个，为了提高效率，FPGA采用并行处理的方式，实现在一个时钟周期内，完成对数据包实现所有过滤器遍历。无疑，这样可以极大地提升IPS的处理速度，但必须实现FPGA的并行化。 而协议重组分析是指，所有流经IPS的数据包，首先经过硬件级别的预处理，这个预处理过程主要完成对数据包的重组，以便IPS能够看清楚具体的应用协议。在此基础上，IPS根据不同应用协议的特征与攻击方式，将重组后的包进行筛选，将一些可疑数据包送入专门的特征库进行比对。由于经过了筛选，可疑数据量大大减少，因此可以大幅度减少IPS处理的工作量，同时降低误报率，当然这个预处理的过程将会是重中之重。 McAfee安全顾问陈纲表示，无论采用那种实现方法，获得的效果是类似的。但用户需要关注的是，由于攻击方式的不断增长，过滤器或者特征库会不断增加，因此如果把所有的检测项目都启用，会给IPS性能造成极大挑战，也没有必要。 Juniper技术经理徐洪涛指出，合理的做法是，用户应该根据自己网络的状态，根据系统的寿命，来评估自己日常应用的攻击风险，选择适合自己的检测项目。 对于漏报，TippingPoint网络技术顾问李臻表示目前的主要问题有两点，一是因为过滤器编写粗糙造成的，例如仅

仅是简单的根据特征字符串检索，就难以防御变种攻击 二是在某些繁忙时段，大量深度检测造成IPS设备的处理能力濒临极限，易造成系统混乱，形成漏报或误报 另外，对于用户关心较多的防御DoS攻击的问题，当前主流IPS厂家的做法分为两类（以SYN flood为例）：第一类是采用SYN Proxy（也可以采用SYN Cookie）的方式。在这种方式中，IPS设备中会设置一个SYN Proxy做代理，当外来的TCP SYN需要和企业Web服务器（或者数据库服务器）建立连接的时候，IPS中的SYN Proxy会首先和外来TCP SYN建立连接，同时发送SYN ack帧。如果是真实的外部用户访问，则会回复一个Ack响应帧。
当SYN Proxy收到响应后，就会认为三次握手成功，同时把连接中继给企业的Web服务器；但如果是SYN flood攻击的半开连接，由于没有响应回复，就会被TCP Reset。如果攻击者利用大面积僵尸网络发起攻击，则会存在大量的真实连接，这就要求IPS必须分配给SYN Proxy或SYN Cookie功能模块的处理资源足够多（不可能无限大）。 第二类是采用深度学习方式。首先IPS设备在in line使用前，先作为off line状态进行流量学习。学习的目的是统计分析企业网的正常流量、常见外部访问地址等信息，并将这些信息建立一个散列表。此后将IPS设为正常使用，这样即便遇到大量的僵尸网络攻击，IPS也可以根据日常学习的结果，优先保证常见外部地址的访问，缓解攻击的影响。 Radware资深工程师滕昕表示，对于DoS的防御，用户也要根据自己的实际情况作出选择。如果用户面临的威胁很大，甚至是经常遭受团体攻击行为，则用户需要具有大量CPU周期资源和大量内存空间的IPS或防火墙来应对。因为在IPv4阶段，只有凭借大量的SYN IO能力，才能最大程度

缓解攻击的影响。 破解三 分析“ 集成安全网关 ”随着IPS的不断发展，一种融合了IPS、防火墙、VPN甚至是防病毒功能的产品逐渐流行，这就是所谓的集成安全网关，以Juniper ISG为例，将第四代安全ASIC和可插拔的安全模块结合在一起，而且每个模块都带有自己的处理容量和存储器，可以提供IDP（IDS IPS）、防火墙和VPN功能。此外，像TippingPoint、Fortinet、Symantec也都有类似的产品。 Juniper大中华区新兴技术经理吴若松认为，此类产品对用户的诱惑很大，因为这种产品可以提供安全处理能力与网络分段特性，可以防止蠕虫、特洛伊木马、间谍软件和恶意软件等现有的和新出现的应用层威胁。同时，状态特征和协议异常检测等多种攻击检测机制，使IDP能够深入分析应用协议与上下文状态，以便有针对性地提供应用防护。 Radware资深工程师滕昕表示，一般集成化的产品网络性与易用性都非常优秀，大部分产品都考虑到了简化网络部署的需求，可以将IPS产品和操作系统无缝集成，并充分利用经过验证的互联网特性，如OSPF、BGP、RIPv2等动态路由，通过虚拟路由器实现多个路由域，以及实现NAT、路由、透明部署等功能项。 另外，此类产品一般都支持基于策略的管理，管理软件可以提供逐条规则的精细度与灵活性，企业的网络管理员可以根据各种规则和协议，部署串联或者监听模式。而基于角色的管理允许安全团队将管理权分配给适当人员，让一个团队负责管理IPS组件，而让其他团队负责管理防火墙、VPN等。一般这种管理采用图形化界面，可以快速地进行攻击和事故调查，以及审核与提交报告等工作。 从目前的使用上看，这种产品在新建企业和大型企业的分支机构使用较多，大多分为100Mbps或者1Gbps。

国内用户应当注意的是，选择此类产品一定要结合自身的应用。因为不同产品支持的特性不一样，以集成的防火墙功能为例，一些安全网关只是集成了精简版的防火墙，对于NAT或者动态端口功能并不支持。 因此，如果用户需要在防火墙上做NAT，或者希望采用VoIP实现语音传输，那么就不能选择此类产品。相反的，一些刚建立的企业机构，在内部应用不多的情况下，选用此种产品无疑是划算的。 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个许可证的集成安全网管产品就实现了全球网络的入侵防护，而管理人员只需要3至4人，效率却提高了6倍以上。 破解四 研究“ IPS摆位方案 ”有意思的是，随着IPS产品越来越成熟，性能越来越强大，有种呼声认为，IPS完全可以代替边界防火墙的位置，部署在出口路由器与防火墙之间，作为企业的第一道安全屏障。 从各大安全BBS的反馈看，有关此类问题的争论越演越烈，以至于国外权威的网络与安全测试机构NSS也在报告中对此问题进行了专题讨论。为此，笔者认为有必要与国内用户进行一些经验分享。 以北京大学的IPS部署为例。北大采用了将IPS部署在出口路由器和防火墙之间的策略，其主要目的是为了实现校园网的网络架构防护。 由于校园网的特点，校内路由器、交换机、DNS服务器以及防火墙都是有可能被攻击的网络设备，如果这些网络设备被攻击导致停机，那么所有关键应用也会随之停止。而利用IPS实现网络架构防护机制，则以一系列的网络漏洞过滤器为基础，用来保护网络设备免于遭受攻击。 在此模式中，IPS也必须提供异常流量统计机制的过滤器。这些过滤机制可以

调整与学习IPS所在的特别环境中“ 正常流量 ”的模式。一旦正常流量被设定为基准，这些过滤机制将依据可调整的门限阀值来侦测统计异常的网络流量。对于超过“ 基准线 ”的正常网络流量，可以针对其通信协议或应用程序特性来进行警示、限制流量或阻绝流量等行动。 如此一来，IPS可以预防DDoS、未知的蠕虫、异常的应用程序流量与其他零时差闪电攻击所造成的网络断线或阻塞。此外，一些Hi-End级IPS厂家还可以依据应用程序的种类、通信协议与IP进行最合适网络流量分配。 NSS的报告更加细致，将IPS从传统的主机型（HIPS）和网络型（NIPS），进一步拓展出抗攻击型（Attack Mitigator）。与NIPS以内容为基础（Content-Based）不同，抗攻击型IPS以速率为基础（Rate-Based），将此种IPS部署在防火墙之前，为的就是快速终结DoS与DDoS攻击。McAfee安全顾问陈纲表示，将IPS摆放在防火墙之前，主要还是出于防火墙被流量攻瘫的担忧，毕竟大多数情况下，一旦防火墙被流量冲死，就会造成网络的暂时中断。 用户应该了解的是，这样做也是有条件的：第一，用户的边界防火墙预留性能有限。根据经验，确实有少部分用户采购过自身设计优秀、且拥有大量CPU资源和内存空间的Hi-End级防火墙，对于这类用户，IPS放在哪里并无关系。 第二，用户采购的IPS产品除了有强大的吞吐能力外，产品架构、CPU资源、内存空间也都要有独到的设计。 第三，即便是再强大的设备，如果遇到集群僵尸网络攻击，一般也很难突破500万条的抵抗极限。 主流Hi-End级IPS厂商产品 TippingPoint UnityOne UnityOne是由最新型的网络处理器技术组成的一个高度专业化的硬件式入侵检测防御平台。UnityOne可以提供业界最完

整的入侵侦测防御功能，包括：应用程序防护、网络架构防护与性能保护。这三大功能可以防御各种形式的网络攻击行为，如：病毒、蠕虫、拒绝服务攻击与非法的入侵和访问。UnityOne是唯一荣获IPS/IDS专业测试机构NSS Group所颁发的NSS Gold Award奖项的IPS 设备。 McAfee IntruShield IntruShield提供业界唯一的明文攻击和加密攻击防护，同时依靠专利的检测技术，可以集中化管理，灵活地部署，具有业界最高的千兆级端口密度，使得企业、运营商和服务提供商能够部署最为准确和全面的防护技术，即使网速高达数千兆时也能实时防护攻击。 由于囊括了范围广泛的众多解决方案（从几百兆至数千兆不等），其前瞻性防护可以从网络核心层延伸至边缘和分支机构，并且可以确保业务的可用性及关键资源的安全。 Juniper IDP Juniper IDP提供全面易用的在线保护措施，IDP可以将应用和网络可视性与事件调查和纠正功能集成在一起，以帮助客户快速而自信地部署在线攻击防护功能。 以在线方式部署时，Juniper IDP可以在网络和应用级攻击造成任何损坏前有效地识别并阻止它们，从而最大限度地缩短处理入侵的时间并降低成本。 Radware DefensePro 借助Radware的StringMatch硬件引擎，DefensePro提供了独特的内置安全交换和高速深度包检测，从而确保对所有网路流量进行双向扫描，以便防范应用级别的攻击。DefensePro提供了高速DoS/DDoS防范和高级的SYN flood防范，包括应对所有已知和未知的SYN flood，每秒拦截高达1300000条SYN，从而确保网络免受拒绝服务攻击。 编看编想：部署IPS走效益路线 从大量国内外应用案例分析，笔者认为国内用户在部署IPS的时候，最好采取分阶段、分层次的做法，这样可以获得最大

的经济效益。 第一阶段，用户可以把IPS当作一个传统的IDS使用。毕竟是新设备，从稳定性、处理能力和网络状态方面考虑，建议首先将IPS设备并联接入。 第二阶段，运行一到两周以后，如果用户觉得使用上没有问题了，再进行串联接入，但是不要做任何数据的阻断。这样运行一段时间后，如果IPS性能和检测能力没有问题，用户就可以知道自己网络中经常会发生什么事情了。 第三阶段，在此基础上，实施IPS阻断策略，根据前两阶段的分析，用户可以对感兴趣的攻击进行阻断，从而实现安全防御。 需要注意的是，从设备本身部署过程上划分，这三个阶段并非独立，而是混合的。 比如企业购买一台拥有多个端口的Hi-End级IPS，网络管理员可以在设备某一组端口上做in line，用来管理某一组链路，而在另外一些端口做scan或者其他串联应用，所有的模式混合在一起工作。 特别是一些既有100Mbps端口，又有1GMbps端口的IPS设备，接入到网络以后，用户可以用1GMbps做in line阻断，用100Mbps连接一些新建的网络或者服务器群做scan，检测是否有问题。 另外，在一个IPS端口之下，还可以进一步划分VIPS，每个虚拟IPS中的策略也可以独立配置，这对于国内很多的IDC用户非常有帮助，可以实现逐层对不同网段设置block，对收费用户实施安全LAN控制，对免费用户的LAN就不用做保护。 所以说，分阶段、分层次部署IPS，将会大大提升IPS的使用效益。 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