IPS如何实现深度检测和入侵抵御 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_IPS_E5_A6_82_E4_BD_95_E5_c101_166580.htm 基于策略的安全防御 随着网络攻击技术的不断提高和网络安全漏洞的不断发现，传统防火墙技术加传统IDS的技术，已经无法应对一些安全威胁。在这种情况下，IPS技术应运而生，IPS技术可以深度感知并检测流经的数据流量，对恶意报文进行丢弃以阻断攻击，对滥用报文进行限流以保护网络带宽资源。 IPS如何实现深度检测和入侵抵御 对于部署在数据转发路径上的IPS，可以根据预先设定的安全策略，对流经的每个报文进行深度检测（协议分析跟踪、特征匹配、流量统计分析、事件关联分析等），如果一旦发现隐藏于其中网络攻击，可以根据该攻击的威胁级别立即采取抵御措施，这些措施包括（按照处理力度）：向管理中心告警；丢弃该报文；切断此次应用会话；切断此次TCP连接。 在哪里部署 进行了以上分析以后，我们可以得出结论，办公网中，至少需要在以下区域部署IPS，即办公网与外部网络的连接部位（入口/出口）；重要服务器集群前端；办公网内部接入层。至于其它区域，可以根据实际情况与重要程度，酌情部署。 如何部署 在以下案例中，我们可以看到以IPS为核心的多种网络深度检测/实时抵御的方案；不同的方案，在不同的应用场景当中，可以适当地扩充或简化。 一、 基于策略的安全防御 1. 位于办公网入口的IPS通过应用层协议分析跟踪和特征匹配，发现目的地为业务服务器A的HTTP数据流中隐藏有针对Windows操作系统的DCOM漏洞的恶意利用； 2. IPS将此安全事件上报至管理中心； 3. 管理中

心获取服务器A的基本信息；4. 管理中心根据获取的A的信息，判断该访问是否会造成危害，如果A不运行Windows操作系统或者A确实运行Windows但是已经打了针对DCOM漏洞的补丁，则A是安全的；5. 根据情况，管理中心向IPS下发制定的安全策略；6. IPS执行安全策略，放行或者阻断此次连接请求。 事实上，在这里我们描述的是需要管理中心介入的情况，在一些相对简单的情况下，如果我们事先可以确认服务器集群所运行的操作系统（在90%的情况下这是可能的），那么抵御该网络攻击的规则可以直接施加在IPS上，不再需要与管理中心的交互，从而降低部署的复杂度、提高效率。 二、应用感知的智能防御 1. 办公网用户访问Internet上的WWW服务器；2. IPS检测到该请求，判断该请求符合事先设定的安全策略，放行；3. 该用户与外部服务器的连接建立；4. 该用户试图通过已经建立的连接，利用二次代理，发起对某非法或不良网站的访问请求；5. 根据对应用层协议的深度分析和内容识别，IPS检测到该企图，阻断该次HTTP连接；6. 上报该安全事件到管理中心备查；7. IPS可以根据管理中下发的策略，对该用户进行一定时间的惩罚（拒绝该用户后续的上网请求）。 三、行为分析的智能防御，阻止病毒、蠕虫泛滥 1. 某办公网用户通过公共区域网络访问业务服务器集群；2. 正常连接建立后，位于服务器集群前端的IPS检测到来自该用户的通信流量中隐藏有某种病毒的行为特征，立即阻断该用户的此次访问，并且上报该安全事件给管理中心；3. 管理中心分析该安全事件，根据报文信息定位到该用户，并且制定新的安全策略；4. 接入管理更改该用户的安全等级，下发更新的安全策略给相关网络设备；5. 更新了安全策略的网络设备将该

用户隔离至某特定区域，避免该病毒感染其他网络用户，并采取后续行动。 IPS深度检测与入侵抵御的关键技术 高性能、高可靠性的硬件平台 依赖于对网络设备体系架构的深刻理解和强大的设计开发能力，华为3Com为IPS产品设计了专用的高性能硬件平台。该平台彻底抛弃了目前市面上常见的工控机架构。 协议分析与跟踪技术 通过前面的分析，我们可以看到协议分析与跟踪对IPS设备的重要性。与传统防火墙不同的是，IPS不但要分析和跟踪IP、ICMP、UDP、TCP这几种网络层、传输层的协议，而且，还要对HTTP、HTTPS、FTP、TFTP、SNMP、Telnet、SMTP、POP、DNS、RPC、LDAP、ICQ、MSN、Yahoo Messenger等众多的应用层协议进行分析、跟踪。没有对网络协议和操作系统的深刻理解，要完成这件工作是不可能的。华为3Com已经具备了在操作系统的内核级别对应用协议进行全面跟踪、深度分析的实力；而且，在引入网络处理器后，所有的逻辑检测和协议分析、跟踪都要下移到网络处理器中，采用微码实现，进一步提高系统性能。 特征匹配的性能 从海量的数据中去寻找一定的特征，在计算领域，这历来是一个高计算量、高复杂度的问题；而IPS的报文内容识别，恰恰要基于此工作。那么，如何解决这个CPU杀手和提高设备性能之间的矛盾呢？ 华为3Com采用专用的硬件加速卡来解决这个问题。基于专门的内容查找芯片设计的硬件加速卡在系统中与CPU、网络处理器协同工作，在需要对报文进行内容搜索的情况下，为CPU和网络处理器卸载负担，使得CPU和网络处理器可以专注于报文处理和逻辑检测，从而将内容搜索对系统效率的影响降至最低。目前华为3Com设计的硬件加速卡，可以在千兆的环境下线速地

处理流量。 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