新一代安全防御技术—IPS 的研究①

Research of New Generation Safety Defense Technique: IPS

陶利民　（杭州师范学院 310036）
廖新飞　（温州职业技术学院 325035）

摘要：IPS 是一种既能发现入侵行为、又能阻止入侵行为的新一代安全防御技术。本文先分析了 IPS 的工作原理及体系结构，然后对 IPS 进行分类，并将 IPS 与 IDS 进行了比较，最后介绍了 IPS 的特征。

关键词：安全　入侵　IDS　IPS

1　引言

为了应对各种不同的网络攻击，人们引入了入侵检测系统（Intrusion Detection System，IDS）。入侵检测是通过从计算机网络或计算机系统中的关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和遭到袭击的现象的一种安全技术。不过，入侵检测系统也存在有很大的问题，一是它只能检测攻击，而不能阻止攻击。二是存在较高的漏报率和误报率。随着入侵事件的不断增加和黑客攻击水平的不断提高，传统的防火墙或入侵检测技术已经无力应对，这就需要引入一种全新的安全防御技术—入侵防护系统（Intrusion Prevention System，IPS）。IPS 能完整检测所有通过的数据包，实时决定准许访问通过还是进行阻截。IPS 可配置于网络边界，也可配置于内部网。IPS 就是一种既能发现入侵行为、又能阻止入侵行为的新的安全防御技术。

2　IPS 的工作原理及体系结构

IPS 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。IPS 以串联的方式接入网络中，在交换机或防火墙在运行的过程中，将各种数据流的信息上报给安全设备，IPS 系统可根据上报信息和数据流内容进行检测，在发现网络安全事件的时候，进行有针对性的动作，并将这些对安全事件反应的动作发送到交换机或防火墙上，由交换机或防火墙来实现精确端口的关闭和断开。IPS 技术既有监测的功能，又有主动响应的功能，力求做到一旦发现有攻击行为，立即响应，主动切断连接。IPS 实现实时检查和阻止入侵的原理在于 IPS 拥有数目众多的过滤器，能够防止各种攻击。当新的攻击手段被发现之后，IPS 就会创建一个新的过滤器，IPS 的工作原理如图 1 所示。

IPS 可以对数据包进行检查并阻止恶意内容的前进，从而阻止网络攻击活动。IPS 首先对来自网络的每个数据包，根据报头和流信息对其进行分类；然后，根据数据包的分类，硬件检测引擎中相关的过滤器检查数据包的流状态信息，此时，所有相关过滤器都是并行使用的，如果任何数据包符合异常信息的匹配要求，则该数据包就被标为命中，被标为命中的数据包将被丢弃，与之相关的流状态信息也会更新，系统丢弃该流中剩余的所有内容。

IPS 具有高效的检测机制，IPS 中设置的过滤器，是 IPS 的一个重要部件，它用于锁定针对各类系统弱点的攻击活动。当发现新的系统弱点，IPS 可创建并增加一个过滤器，任何针对系统弱点的恶意操作都会被即时

① 杭州师范学院科研基金项目

阻止。IPS 能进行完整的数据监测，检测各类针对第 2 层到第 7 层的弱点攻击。传统的防火墙仅限于第 3 或第 4 层监测，无法检测到针对应用层的攻击，因为这类

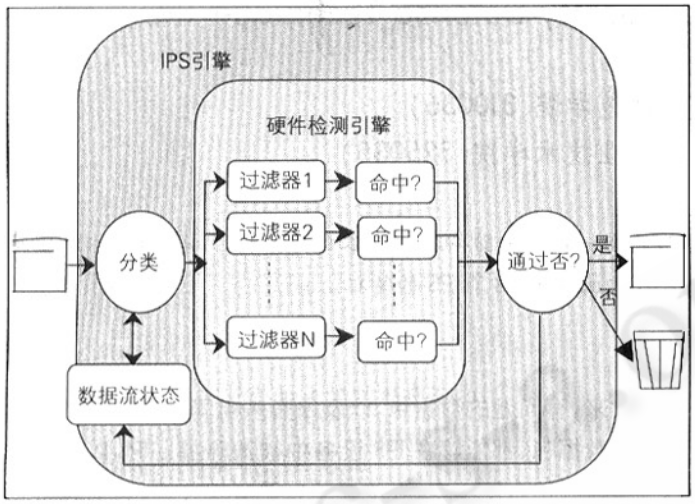

图 1　入侵防护系统工作原理

攻击隐藏于有效载荷中。IPS 的包处理引擎能对数据包中的比特流进行完整监测。随后，IPS 便依据策略分配过滤器，在每次数据流到达时，进行完整的内容检测。

IPS 的体系结构如图 2 所示。IPS 一般采用 ASIC、FPGA 或 NP（网络处理器）等硬件设计技术实现网络数据流的捕获，检测引擎综合特征检测、异常检测、DoS 检测、缓冲区溢出检测等多种手段，并使用硬件加速技术进行深层数据包分析处理，能高效、准确地检测和防御已知、未知的攻击及 DoS 攻击。同时，实施多种响应方式，如丢弃数据包、终止会话、修改防火墙策略、实时生成警报和日志记录等，突破了传统 IDS 只能检测不能防御入侵的局限性，提供了一个完整的入侵防护解决方案。具体来说，IPS 用应用层代理引擎技术解决漏报误报率问题，用引擎硬件化技术解决性能问题。引擎硬件化可大大提升性能，也就是说，IPS 把最消耗资源的部分用硬件实现，把最具有灵活性的部分用软件实现，达到提高性能的目的。

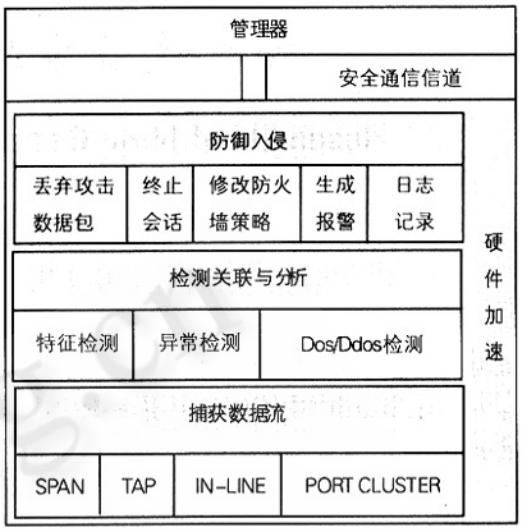

图 2　IPS 体系结构

3　IPS 的分类

3.1　按照信息源分类

根据信息的来源进行分类，IPS 可以分为基于主机的入侵防护（HIPS）、基于网络的入侵防护（NIPS）及应用入侵防护（AIP）。

（1）基于主机的入侵防护（HIPS）。HIPS 通过在主机/服务器上安装软件代理程序，防止网络攻击入侵操作系统以及应用程序。基于主机的入侵防护能够保护服务器的安全弱点不被不法分子所利用。基于主机的入侵防护技术可以根据自定义的安全策略以及分析学习机制来阻断对服务器、主机发起的恶意入侵。HIPS 可以阻断缓冲区溢出、改变登录口令、改写动态链接库以及其他试图从操作系统夺取控制权的入侵行为，整体提升主机的安全水平。

由于 HIPS 工作在受保护的主机/服务器上，它不但能够利用特征和行为规则检测，阻止诸如缓冲区溢出之类的已知攻击，还能够防范未知攻击，防止针对 Web 页面、应用和资源的未授权的任何非法访问。HIPS 与具体的主机/服务器操作系统平台紧密相关，不同的平台需要不同的软件代理程序。HIPS 将朝着集杀毒、防黑和数据安全保密于一体的方向发展，并最终成为一个综合的主机防护解决方案。

（2）基于网络的入侵防护（NIPS）。NIPS 通过检测流经关键网段或交换部位的网络流量，提供对网络系统的安全保护。由于它采用在线连接方式，所以一旦辨识出入侵行为，NIPS 就可以去除整个网络会话，而不仅仅是复位会话。同样由于实时在线，NIPS 需要具备很高的性能，以免成为网络的瓶颈，因此 NIPS 通常被

设计成类似于交换机的网络设备，提供线速吞吐速率以及多个网络端口。

NIPS 必须基于特定的硬件平台，才能实现千兆级网络流量的深度数据包检测和阻断功能。这种特定的硬件平台通常可以分为三类：一类是网络处理器（网络芯片），一类是专用的 FPGA 编程芯片，第三类是专用的 ASIC 芯片。NIPS 的实时检测与阻断功能很有可能出现在未来的交换机上。随着处理器性能的提高，每一层次的交换机都有可能集成入侵防护功能。

（3）应用入侵防护（AIP）。应用入侵防护（Application Intrusion Prevention ，AIP）是 NIPS 的一个特例，它把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设备。AIP 被设计成一种高性能的设备，配置在应用数据的网络链路上，以确保用户遵守设定好的安全策略，保护服务器的安全。NIPS 工作在网络上，直接对数据包进行检测和阻断，与具体的主机/服务器操作系统平台无关。

3.2 按照分析方法分类

根据分析方法，IPS 可分为两大类：特征比对入侵防护系统和异常探测入侵防护系统。

（1）特征比对入侵防护系统。特征比对入侵防护系统的工作原理是将通过的网络业务流与已知的攻击特征进行比对，如果匹配则认为该网络业务流可能为恶意攻击。基于状态的特征匹配不但检测攻击行为的特征，还要检查当前网络的会话状态，避免受到欺骗攻击。特征比对入侵防护系统首先对标识特定入侵的行为模式进行编码，建立入侵特征知识库，然后对实际检测过程中得到的审计事件数据进行过滤，检查是否包含入侵行为的标识特征。特征匹配是最广泛应用的技术，具有准确率高、速度快的特点。

（2）异常检测入侵防护系统。异常检测入侵防护系统的工作原理是学习正常的网络业务流特征，当发现通过的网络业务流与正常业务流有较大变化时，发出警报并采取相应措施，这样可以有效地拦截诸如 DoS 和 DDoS 类型的攻击。异常检测入侵防护系统假定所有的入侵活动都必须是异常的，先建立起所保护的系统的正常情况下的特征轮廓，然后检测偏离特征正常值的情况发生，如果有，则认为可能发生了入侵。异常检测的误报率比较高，IPS 不将其作为主要技术。

4 IPS 与 IDS 比较

IPS 与 IDS 尽管只有一个字母的差别，不过它们的区别还是很大的。从以下三个方面将 IPS 与 IDS 进行比较。

（1）功能方面。IPS 与 IDS 本质的区别在于，IDS 只能检测攻击并报警，是被动防御技术；而 IPS 不仅检测，还能有选择地阻断攻击，是一种主动防御的技术。从功能上来看，IDS 是一种并联在网络上的设备，它只能被动地检测网络遭到了何种攻击，它的阻断攻击能力非常有限，一般只能通过发送 TCP reset 包或联动防火墙来阻止攻击。而 IPS 则是一种主动的、积极的入侵防范、阻止系统，它部署在网络的进出口处，当它检测到攻击企图后，它会自动地将攻击包丢掉或采取措施将攻击源阻断。IPS 专注于提供前瞻性的防护，其设计宗旨在于预先拦截入侵活动和攻击性网络流量。

（2）接入方式。IPS 注重接入控制，而 IDS 则进行网络监控。与 IDS 相比，IPS 增加了在线（In－line）连接和流量阻断两个新特征。在线连接意味着 IPS 成为所监控网络流量的必经之路，而不再像 IDS 那样只是旁路监听流量。此外，IPS 具有 IDS 所不具有的允许或拦截流量的能力。IPS 的接入方式使之成为网络基础结构的一部分，既能实时监视入侵还能实时阻止入侵，提供主动式的安全保障。

（3）误报和漏报。由于能够实时检测和实时阻止攻击，IPS 大大提高了安全保护的效率和效果。由于采用与 IDS 相同的检测技术，IPS 同样面临误报和漏报的风险。但是，两者在出现误报和漏报的后果不一样。在发现入侵时，IPS 需要当即立断作出准许或阻止数据包通过的判断，因此 IPS 的误报和漏报会导致比 IDS 更为严重的后果。IDS 的误报最多只会增加网络噪音，给网管员增加麻烦，然而 IPS 的误报则会导致拒绝服务，合法访问被拒之门外。所以 IPS 减少误报和漏报的需求要比 IDS 更加迫切。

5 IPS 的特征

一个理想的入侵防护系统应该具有以下特征：

（1）主动、实时预防攻击。IPS 解决方案应该提供对攻击的实时预防和分析。它应该在任何未授权活动开始前找出攻击，并防止它进入重要的服务器资源。

（2）嵌入式运行 。只有以嵌入模式运行的 IPS 设备才能够实现实时的安全防护，实时阻拦所有可疑的

数据包，并对该数据流的剩余部分进行拦截。

（3）深入分析和控制。IPS 必须具有深入分析能力，以确定哪些恶意流量已经被拦截，根据攻击类型、策略等来确定哪些流量应该被拦截。

（4）入侵特征库。高质量的入侵特征库是 IPS 高效运行的必要条件，IPS 还应该定期升级入侵特征库，并快速应用到所有传感器。

（5）高效处理能力。IPS 必须具有高效处理数据包的能力，对整个网络性能的影响保持在最低水平。

（6）可扩展性。企业级入侵防护解决方案必须可升级，以满足企业不断发展的需求，而同时保持最高水平的安全。可扩展性体现在可支持众多受保护的服务器、支持大流量和支持分散型安全管理，以满足大型分散式企业的需求。

（7）可靠性和可用性。实时在线设备一旦出现故障，就会关闭某个关键的网络路径，造成拒绝服务。IPS 必须具有出色的冗余能力和故障切换机制，确保不会成为网络部署中的单点故障点。

6 结束语

IPS 有其很大的优势，不过，IPS 技术也面临很多挑战，其中主要有三点：一是单点故障，二是性能瓶颈，三是误报和漏报。设计要求 IPS 必须以嵌入模式工作在网络中，而这就可能造成瓶颈问题或单点故障。如果 IDS 出现故障，最坏的情况也就是造成某些攻击无法被检测到，而嵌入式的 IPS 设备出现问题，就会严重影响网络的正常运转。如果 IPS 出现故障而关闭，用户就会面对一个由 IPS 造成的拒绝服务问题，所有客户都将无法访问企业网络提供的应用。不过，IPS 的不足并不会成为阻止人们使用 IPS 的理由，因为安全功能的融合是大势所趋，入侵防护顺应了这一潮流。

参考文献

1 戴英侠、连一峰、王航，系统安全与入侵检测[M]，北京 清华大学出版社，2002。

2 Intrusion Prevention Systems (IPS) Next Generation Firewalls [EB/OL]. http://www.bitpipe.com/detail/RES/1080065083_31.html,2006-1-7.

3 Intrusion Prevention Systems complete security [EB/OL]. http://www.networkworld.com/edge/columnists/2002/1016bleed.html,2006-1-7.