一种分布式网络入侵防御系统①

薛　辉[1]，邓　军[2]，叶柏龙[3,4]，陆　兰[3]

[1](湖南涉外经济学院，长沙 410205)
[2](湖南科技职业学院，长沙 410004)
[3](中南大学，长沙 410083)
[4](湖南创博龙智信息科技股份有限公司，长沙 410205)

摘　要：为了改进当前 IPS 面临性能瓶颈、误报、漏报和攻击速度等问题，提出了一种分布式“分析与检测＋集中控制＋升级服务”架构的网络入侵防御系统。分析与检测主要采用协议识别和分析、协议异常检测、流量异常检测及响应方式等，集中控制主要用于监测控制入侵检测与防御系统的运行及其系统配置，升级服务负责定期提供攻击特征库的升级更新，使系统提供最前沿的安全保障。同时兼容其他安全产品，形成深度防御体系，最大限度地保护企业和组织的网络安全。

关键词：入侵检测与防御；协议识别；异常检测；流量监测；网络攻击

A Distributed Network Intrusion Prevention System

XUE Hui[1], DENG Jun[2], YE Bai-Long[3,4], LU Lan[3]

[1](Hunan International Economics University, Changsha 410205, China)
[2](Hunan Vocational College of Science and Technology, Changsha 410004, China)
[3](Central South University, Changsha 410083, China)
[4](Hunan BLRise Information Technology Co. LTD, Changsha 410205, China)

Abstract: In order to improve the current performance bottlenecks facing IPS, false positive, false negative and attack speed issue etc, this paper presents a distributed “analysis and testing+centralized control+upgrade services” Architecture for Network Intrusion Detection and Prevention System. Analysis and testing can be achieved mainly through protocol identification and analysis, protocol anomaly detection, traffic anomaly detection and response methods. Centralized control is primarily used for intrusion detection and prevention monitoring and control system operation and system configuration. Upgrade Service is responsible for regular upgrades attack signature updates to make sure that the system provides the most cutting-edge security. Compatible with other security products, this system forms the depth of defense, to protect businesses and organizations to maximize network security.

Key words: intrusion detection and prevention; protocol identification; anomaly detection; flow monitoring; network attacks

目前随着信息化建设的蓬勃发展，国家对网络安全给予了高度重视。网络入侵防御系统（IPS）技术发展也相当迅速，它能够以更细粒度的方式检查网络流量，主动地对安全事件进行响应，防止各个层面攻击事件的发生。但是，目前的 IPS 仍然面临着一些问题：

1）性能瓶颈[1]：即使 IPS 不出现故障，由于需要处理所有的网络流量和系统调用，必然会增加滞后时间，这样就可能导致网络和系统效率的降低，使之成为一个潜在的性能瓶颈。

2）误报和漏报[2]：如果产生误报将会导致合法的流量或者请求被意外拦截，形成拒绝服务。对于实时在线的 IPS 来说，一旦拦截了攻击性数据包，就会对

① 基金项目:国家改委信息安全产品专项基金(发改办高技[20091886 号])
收稿时间:2011-01-20;收到修改稿时间:2011-02-23

来自可疑攻击者的所有数据流进行拦截。如果产生漏报，将会导致攻击事件的成功发生。

3) 攻击工具越来越先进[3]：现在的攻击工具具备了反侦破和动态行为，可以绕过防火墙，且不对称攻击的威胁在不断扩大。

4) 攻击的自动化程度和速度不断提高，且杀伤力逐步增强。发现安全漏洞越来越快，覆盖面越来越广，新发现的安全漏洞每年要增加一倍，而且安全漏洞类型不断翻新。

为了解决上述问题，我们在 IPS 架构设计及系统实现上进行了深入的研究，针对目前流行的蠕虫、病毒、间谍软件、垃圾邮件、DDOS 等黑客攻击，以及网络资源滥用，提出一种分布式“分析与检测＋集中控制＋升级服务” 技术架构的网络入侵防御系统(以下简称 DNIPS)。该系统的特点体现在高度融合性、高安全性、高可靠性和易操作性等特性，能自动对各类攻击性的流量，尤其是应用层的威胁进行实时阻断。

1 DNIPS研究

1.1 DNIPS 概述

针对目前的 IPS 主要问题，在参考了大量国内外 NIPS 技术的设计思想之后，在性能瓶颈方面采用的快速模式匹配算法进行攻击特征匹配[4]，用于提高系统检测效率，减少滞后时间。在误报和漏报方面融合基于 CSD 的协议异常检测方法[5]、基于因果关系和知识积累的告警相关方法，基于序列比对的攻击特征自动提取方法[6]，从不同角度，各种方法取长补短提高系统攻击特征质量，减少误报率和漏报率。针对攻击工具和攻击速度方面，采用实时监测和及时自动升级方式，方便在各种网络环境中灵活部署和管理。使系统具备深度入侵防御、精细流量控制等功能，为用户带来深度攻击检测与防御。

1.2 DNIPS 关键技术分析

1）协议识别和分析。本系统采用智能协议识别技术，特点在于可以通过动态分析网络报文中包含的协议特征，发现其所在协议，然后递交给相应的协议分析引擎进行处理，高速、准确地检测出通过动态端口或智能隧道实施的恶意入侵，及时准确的发现绑定在任意端口的各种木马、后门，即使运用智能隧道技术的软件也能准确捕获和分析，通过实验采样分析，该技术能够全面识别超过 100 种以上的应用层协议[7]。

2）协议异常检测。采用基于 CSD 异常检测技术；该技术是基于马尔可夫链模型检测协议异常的有效性，可通过分析更多数据以确定采样窗口、阀值以及 W 的优先值；还可对加密协议进行协议异常检测。对常见的检测检查特定应用执行缺陷（如：应用缓冲区溢出异常），或者违反特定协议规定的异常（如：RFC 异常）都可实施防范。该技术较基于误用检测技术来说，可以避免在产品升级的时间间隔内无法检测到黑客的该攻击行为[5]。

3）流量异常检测。采用基于路由变化、流变化和包延迟，以及 IP 报文头信息(例如 TTL、源/目的地址、报文长度和路由器时间戳)建立网络行为模型，通过学习和调整特定网络环境下的“正常流量”值，来发现非预期的异常流量。一旦正常流量被设定为基准(baseline)，系统会将网络中传输的数据包与这个基准作比较，如果实际网络流量统计结果与基准达到一定的偏离，则产生警报。流量异常检测和过滤机制使得系统可以有效抵御分布式拒绝服务攻击(DDOS)、未知的蠕虫、流氓流量和其他零日攻击。

4）DOS 攻击检测。通过分析典型拒绝服务攻击例如 Smurf、SYN Flooding、UDP Flooding 和 ICMP Flooding 等，以及典型拒绝服务攻击工具（例如 Tribal Flood Network、Trin00、TFN2K 和 Stacheldraht），提取拒绝服务攻击特征，可设计一个拒绝服务攻击检测模块，阻挡或限制未经授权的应用程序触发的带宽消耗，极大限度地减轻 DOS 攻击对网络带来的危害。

5）响应方式。采用丢弃数据包、中断连接、邮件报警、短信报警、控制中心显示、日志数据库记录、写入 XML 文件、打印机输出，运行用户自定义命令等多种响应方式，同时提供标准 snmp trap（V1、V2、V3）和 syslog 接口，用于接受第三方管理平台的安全事件集中监控、报告和管理。

2 DNIPS实现

从系统实现的角度来看，本系统采用 3 个层次、3 个核心模块来实现，系统体系架构如下图所示，下面分别进行论述。

2.1 DNIPS 层次架构实现

从层次结构上看，本系统分为 3 个层次来实现：

1）软件升级层

该层设计一个升级模块，为用户提供升级服务，

每周定期提供攻击特征库的升级更新，若在紧急情况下还可提供即时更新，使系统提供最前沿的安全保障。

2）中心控制层

主要用于监测和控制系统的运行及其系统配置，管理各种日志的分析、归并、备份和回复，以及入侵检测的特征库、防火墙安全策略(主要指访问控制策略)等。并同时管理 B/S 和 C/S 两种系统，采用 Web 方式，方便灵活管理，以便适合在任何 IP 可达地点远程管理，真正意义上实现跨平台。

3）系统检测与防御层

是本系统的核心层，该层以智能协议识别技术为基础，融合协议异常检测、流量异常检测、告警相关分析，以及防火墙协作等多种技术。对控制的系统从多角度、全方位，主动、综合、协同和一体化方向考虑，对网络进行多立体、纵深、动态防护。

此外要求凡是进入本系统的协议或数据都必须基于统一标准，均以规范的形式提供服务；各层次间数据传输均要求经过高强度的 SSL 安全通道，进一步保证信息在网络中的传递安全。

2.2 DNIPS 模块实现

从模块结构来看，3 个核心模块可实现本系统的主体功能，这些模块根据层次的划分而分解为多个子模块，每个子模块根据其特点划分到系统的不同层次，3 个核心模块的功能如下：

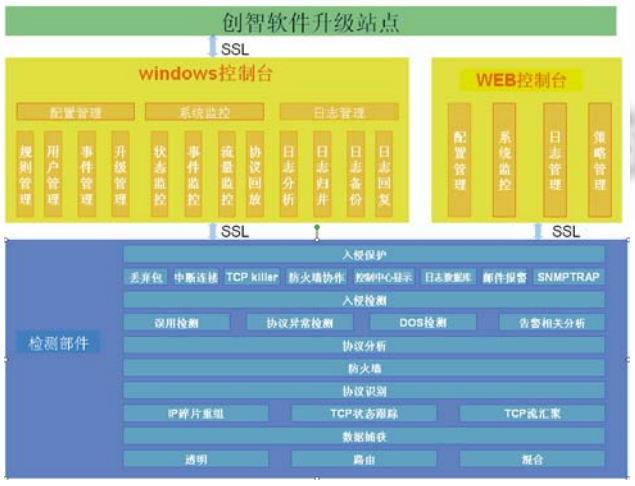

图 1　DNIPS 体系架构图

1）windows 控制台模块

该模块主要针对 C/S 架构的应用系统提供服务。分为配置管理、系统监控和日志管理 3 个子模块，其中配置管理主要用于规则管理、用户管理、事件管理和升级管理；系统监控主要对事物的状态、事件的发生、流量的变化和协议的回放进行监控；日志管理主要对日志的分析、日志的归并、日志的备份和日志的回复进行管理。

2）WEB 控制台模块

该模块主要针对 B/S 架构的应用系统提供服务。分为配置管理、系统监控、日志管理和策略管理 4 个子模块，前面 3 个子模块跟 windows 控制台模块相似，根据 B/S 架构应用系统的特征增加策略管理，采用自定义访问控制策略，用于根据不同事态变化，对各种策略进行综合评估和分析，采取相应的策略进行检测或防御。

3）系统检测模块

该模块位于系统检测与防御层，是本系统的核心模块。主要包括入侵保护、入侵检测、协议分析、防火墙、协议识别和数据捕获 6 个子模块。其中入侵保护主要对包的丢失、中断连接、TCP killer、防火墙协作、邮件报警、SNMPTRAP、和日志数据库等进行保护及响应。入侵检测主要采用 CSD 的协议异常检测技术和设计一个拒绝服务攻击检测模块，对误用、协议异常和 DOS 的检测进行相关分析，并通过告警系统及时响应；协议分析主要采用智能协议识别技术，通过动态分析网络报文中包含的协议特征，发现其所在协议，然后递交给相应的协议分析引擎进行处理。防火墙模块对访问控制采用内置状态防火墙和自定义访问控制策略。对 NAT 支持提供网络地址转换功能，支持静态 NAT（Static NAT）、动态 NAT（Pooled NAT）和端口 NAT（PAT），支持多对一、多对多和一对一等多种地址转换方式；在路由方面使用灵活的策略路由功能，根据协议类型、应用、IP 源地址等策略来选择数据转发路径，根据报文数据流的发起方向来确定以后的路由，满足各种应用环境的需要。协议识别主要负责对分析出来的 IP 碎片重组、TCP 状态跟踪和 TCP 流的汇聚进行识别并作出标志。最后是数据捕获，对来自于经过上述模块的分析和识别的数据包进行捕获，获得该数据包的源地址、源端口、目的地址、目的端口和所使用的协议等数据，并进行相关告警，必要时自动关闭网络设备。

通过对系统的层次和模块两个维度的分析和设计形成了本系统的完整实现思路，本系统作为一种在线

部署的产品，其目标不仅仅在于能够精确识别各种黑客攻击，而且必须在不影响正常业务流量的前提下对攻击流量进行实时阻断，而不是在监测到恶意流量的同时或之后才发出告警。弥补了防火墙、入侵检测等产品的不足，为用户提供较全面的安全检测与防御。

3 结语

本系统是在响应国家“信息安全”产品产业化专项基金的要求下，旨在研发出一种能自动采取行动阻止攻击和入侵，这种分布式“分析与检测＋集中控制＋升级服务”技术架构的网络入侵防御系统弥补了当前 IPS 的不足。通过部署该入侵防御系统，同其他安全产品形成互补，形成深度防御体系，最大限度地保护企业和组织的网络安全。目前本系统已经通过国家发改委验收，并成功运行在 PowerSEC 高性能监控一体化网络安全平台上，实践证明该系统具有极大的研究价值、开发价值和市场前景。然而，入侵防御技术现在还处于不断完善过程，基于攻击技术和手段还在不断发展变化，仍然需要不断的改进，这样才能更有效地保护网络，这也正是我们后续的研究方向。

参考文献

1 Muk herjee B.Network intrusion detection. IEEE Networks, 2005,23(4):284–285.

2 华睿,李学桥.一种基于 Linux 的网络入侵检测系统.郑州轻工业学院学报(自然科学版),2005,1(1):44–46.

3 O’Neill LT. IDS vs. IPS Explained.May 29th,2007. http://www.networksecurityjournal.com/features/ids-vs-ips-052907/

4 Huang K. An Approach To Generating Testing Traffic In Evaluating Network Intrusion Detection Systems. Proc. of Systemics, Cybernetics and Informatics (SCI2004). July 2004, Orlando, USA.

5 秦拯,李娜,张大方,邹建军.Chi-square Distance 在协议异常检测中的应用.湖南大学学报(自然科学版),2005,32(4):99–103.

6 秦拯,尹毅,等.基于序列比对的攻击特征自动提取方法.湖南大学学报(自然科学版),2008,35(6):77–81.

7 邵颖佳,张大方,黄昆.无线自组织网络中动态源路由协议的移动性分析.计算机应用研究,2007,24(9):212–213.

(上接第 64 页)

ation Aggregation in Sensor Networks. Proc. of the first ACM Conference on Embedded Networked System, New York: ACM Press, 2003.255–265.

10 Zhu YJ, Vedantham R, Park SJ. A Scalable Correlation Aware Aggregation Strategy for Wireless Sensor Networks. Proc. of IEEE International Conference on Wireless Internet(WICON). Budapest, 2005.

11 Wei Y, Krishnamurthy SV, Tripathi SK. Synchronization of Multiple Levels of Data aggregation in Wireless Sensor Networks. Proc. of Global Telecommunications Conference. 2003.223–225.

12 王结太,许家栋,于海勋.分组敏感的无线传感器网络实时数据融合树算法.传感技术学报,2008,21(10):1760–1764.

13 李敏,罗挺,周俊.WSN 中基于虚拟锚节点的 AD 定位算法研究.后勤工程学院学报,2010,(6):45–49.

14 王洋.基于动态半径的事件驱动型无线传感器网络分簇融合算法.电子测试,2009,12(12):1–6.

15 袁凌云,王兴超,赵艳芳.基于事件驱动和最小延迟融合路径的无线传感器网络突发事件监测研究.传感技术学报,2009,22(9):1312–1317.

16 雷昕,鄢楚平,徐海川.无线传感器网络数据融合技术的研究与仿真.计算机工程与设计,2008,18(9):4669–4671.