千兆线速入侵检测系统的设计与实现*)

徐陈佳　蔡圣闻　谢俊元　陈世福

(南京大学软件新技术国家重点实验室　南京 210093)

摘　要　随着千兆网络开始在国内大规模普及,对千兆线速入侵检测系统等高性能网络安全产品的需求日益迫切。本文基于 IXP2400、pp1200、TCAM 芯片和 CPCI 2.16 技术开发了千兆线速入侵检测系统硬件平台,并基于该平台设计并实现了一个千兆线速级入侵检测系统。该入侵检测系统较之用网络处理器(NP)和专用集成电路(ASIC)技术实现的千兆入侵检测系统具有结构开放、灵活,综合计算能力强,可靠性高等优势。

关键词　千兆,线速,入侵检测,网络扫描检测

Design and Implementation of Kilomega Wirespeed Intrusion Detect System

XU Chen-Jia　CAI Sheng-Wen　XIE Jun-Yuan　CHEN Shi-Fu

(National Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)

Abstract　With the popularization of the kilomega wirespeed network, kilomega wirespeed intrusion detect system(ids) becomes necessary. Based on Xpeedium™ CXE-16, pp1200, TCAM chip, CPCI 2.16 technique, we propose a universal hardware platform, and design and implement a kilomega wirespeed intrusion system on the platform. Compared to those system based on NP or ASIC our system is good at structure, flexibility, computation, reliability.

Keywords　Kilomega, Wirespeed, Intrusion detect system, Network scan detection

1　引言

目前正处于由百兆网络向千兆网络过渡的时期,网络环境有了很大的变化,传统的百兆网络入侵检测系统已经不能再适应新时期的要求了。从百兆网络到千兆网络这种网络传输性能的提高,对传统入侵检测技术的冲击是全方位的,例如要实时处理的数据流的增大,对网络延时要求的提高。面对高速网络环境对安全保障提出的新的要求,以及环境中新的安全威胁,传统的入侵检测系统的硬件平台技术变得不再适用。

目前的入侵检测系统大都基于 PC 架构,UNIX 平台,从 CPU 频率到系统处理能力都存在瓶颈,而一些使用网络处理器技术[1]和 ASIC 技术的千兆入侵检测系统,在需要对大量的应用报文数据内容进行分析检查的时候,会导致单独使用 ASIC 芯片加速技术或 NP 的系统性能急剧下降。该系统基于 IXP2400、pp1200、TCAM 芯片和 CPCI 2.16 技术开发了千兆线速入侵检测系统硬件平台[2,3],利用 IXP2400 采集网络数据,再根据负载均衡的原则将数据分配到多个 X86 处理板上进行检测,用基于哈希链表的方法来检测网络扫描,采用更为完整详细的协议分析,大大提高了系统的效率,提高了性能,还对报警事件进行了分类,按类别报警,有效地缓解了事件风暴问题。

下面就介绍该系统,在第 2 节中介绍千兆线速入侵检测系统的硬件平台,在第 3 节中介绍系统的软件系统结构,第 4 节介绍系统的关键技术,第 5 节介绍系统的测试结果,最后进行了总结。

2　千兆线速入侵检测系统的硬件平台

该系统的硬件平台主要由 IXP 2400、pp1200、TCAM 芯片组成,并采用了 CPCI 2.16 技术,下面将介绍它的结构、平台处理流程。

2.1　平台硬件结构

整个硬件平台由 4 个部分组成:

1. 支持 CPCI 2.16 的机箱,包括冗余电源、系统硬件故障自检单元;

2. 基于 CPCI 2.16 的系统内部数据交换支持系统,提供带宽最高可达 32Gbitps 的数据交换支持;

3. 支持 CPCI 2.16 的 X86 架构的数据处理和存储板卡;

4. 支持 CPCI 2.16,并能提供千兆线速接入和转发处理能力的接入和前端预处理板卡(以下简称接入板),该板卡集成了多个千兆光纤和 RJ45 网络接口。

其中接入板是整个硬件平台系统的关键。接入板的设计采用 Intel 的 IXP2400 网络处理器,并集成支持高速查表的 TCAM 芯片和支持对内容进行模式检查、匹配和标记的 PP1200 芯片、CPCI2.16 接口控制芯片,以及基于 FPGA 开发的协调 IXP2400、PP1200 和 TCAM 协同工作的控制器。

2.2　平台处理流程

该平台系统的数据处理流程图如图 1 所示。

其具体的数据包处理流程描述如下:

1. 网络数据包传送至数据处理平台的外接口;

2. 接入数据处理板对数据进行第一层次的分析,判断数据的合法性,判断内容主要包括:数据包是否是正常的数据

*)本文得到国家自然科学基金(6050302)和江苏省科技厅高技术研究资助项目(BG2005029、BG2006027)资助。徐陈佳　硕士研究生,主要研究领域为计算机网络、信息安全;蔡圣闻　博士研究生,主要研究领域为计算机网络、信息安全;谢俊元　教授,博士生导师,主要研究领域为人工智能、信息安全;陈世福　教授,博士生导师,主要研究领域为分布式人工智能、大型知识库和数据库以及图像处理。

包、是否满足接入数据处理板的过滤规则[4]；

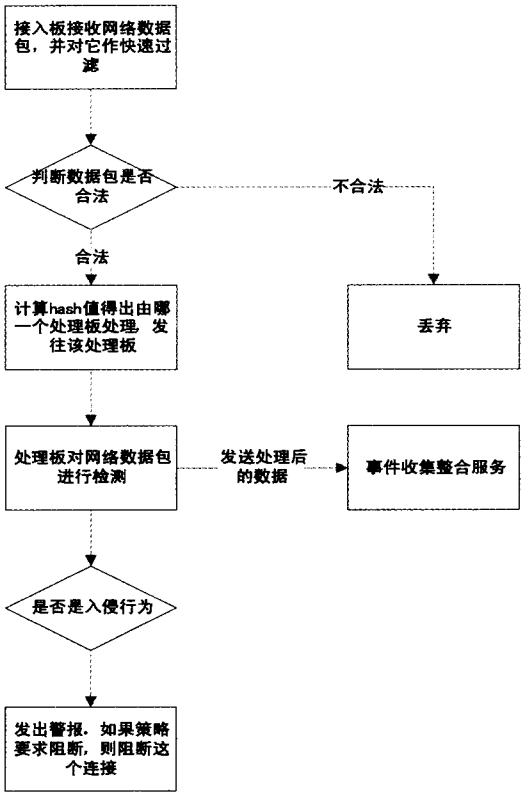

图 1　硬件平台数据处理流程图

3. 如果数据包不满足接入数据板的合法性过滤规则，则该数据包被丢弃；

4. 如果数据包满足接入数据板的合法性过滤规则，则依据该数据包的源 IP 地址源端口进行 Hash[5]，将数据包转发到与 Hash 值相对应的后接 X86 数据处理存储板上进行入侵检测；

5. 每个 X86 处理板对分配到的网络数据连接进行整理，包括 IP 分片重组，TCP 流重组等，同时进行入侵检测，判断是否是入侵行为，如果是，则向控制台发出报警，如果策略还要求对这个数据连接进行阻断，那么就发送消息给防火墙，防火墙负责将数据连接阻断。整理后的网络数据都将被发送到事件收集整合器服务组件，以供以后查询分析。

3　千兆线速入侵检测系统的软件系统结构

3.1　软件系统结构

千兆线速入侵检测系统采用分布式体系结构，整个系统分为两个有机的部分：探测器（硬件平台部分）和控制器。

探测器运行在整个网络的出入口，以及内部网络中需要重点保护的网段；控制器提供远程控制、显示和管理功能。网络探测引擎全面侦听网上信息流，动态监视网络上流过的所有数据包，进行检测和实时分析，从而实时甚至提前发现非法或异常行为，并且执行告警、阻断，记录相应的日志等功能。

控制器是由多个模块构成的高性能的管理系统，主要包括控制台、实时监控和内容恢复模块，以及攻击事件管理，安全策略配置管理，系统配置及用户权限管理模块。

软件系统组成如图 2 所示。

3.2　软件处理方法

在接入板获取网络数据包后，由 X86 处理板对数据包进行 IP 分片重组，TCP 流重组，进行全状态跟踪，判断是否是扫描攻击，拒绝服务攻击，还要进行异常检测[6]。

然后再进行应用层协议分析，看是否有协议异常，并实施安全策略，如阻断 P2P 协议等，继续跟踪协议的状态，同时记录下协议过程，以便以后进行协议恢复。

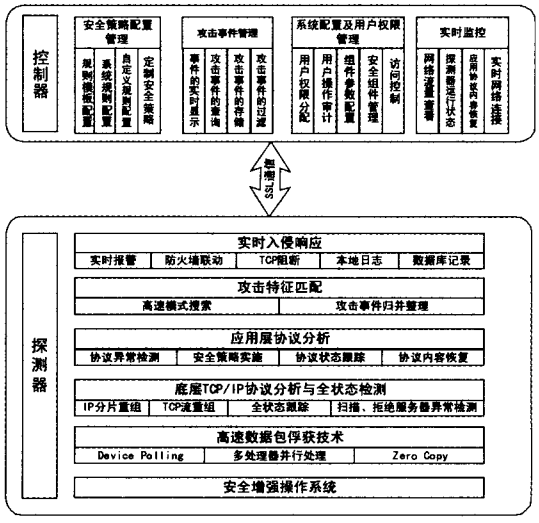

图 2　软件系统结构图

与此同时还会对报文进行攻击特征匹配，如果有攻击事件产生，会对事件进行整理分类，并实时报警，如果策略要求的话，还要通知防火墙进行 TCP 阻断，并把所有信息记录到日志数据库中，以备后来分析。这就是探测器端的主要任务。

在控制器端，可以实时地观察到探测器端探测到的信息，探测器的运行状态，网络流量，还可以对应用层协议进行恢复，再现以前的网络数据。另外控制器还负责系统用户权限的配置，安全策略配置管理，攻击事件管理等。

4　关键技术与实现

该系统的实现主要是使用 IXP2400、pp1200、TCAM 芯片和 CPCI 2.16 技术构造硬件平台采集过滤网络数据包，采用多个 X86 处理板进行入侵检测，达到负载均衡的目的，采用基于哈希链表的网络扫描检测，并对协议分析技术进行了改进，对报警事件进行了分类。下面对一些关键技术作详细的介绍。

4.1　基于哈希链表的网络扫描检测

该系统采用的网络扫描判定方法是：检测在一定时间内，一台主机发起的连接数是否超过了阈值，如果超过了就判定为扫描行为[7]。系统使用一个网络连接哈希链表来统计网络连接的信息，分析网络情况判断是否发生了网络扫描。

哈希链表的数据结构如图 3 所示。

每当一个新的数据包到达时，扫描检测的算法如下：

1）根据它的源 ip 地址计算 hash 值，找到这个 hash 值对应的 src_addr_head，也就找到了对应的 src_addr 链。

2）然后在链中寻找这个 ip，如果找到了直接跳转到 3，如果没有找到，就新建一个 src_addr 的节点，再新建一个从属 src_addr 的 dest_addr_head 哈希链表，计算出目的 ip 的哈希值，新建它的 dest_addr 链，然后类似的建立它的 port_head 哈希链表，port 链。然后转到 5。

3）接着对找到的这个 src_addr 节点作处理，计算目的 ip 地址的 hash 值，在 dest_addr_head 链中找到目的 ip 的 dest_

addr链，在dest_addr链中查找目的ip地址，如果找到了跳转到4，如果没有就建立一个dest_addr节点，再建立对应于这个目的地址的port_head哈希链表，port链。然后转到5。

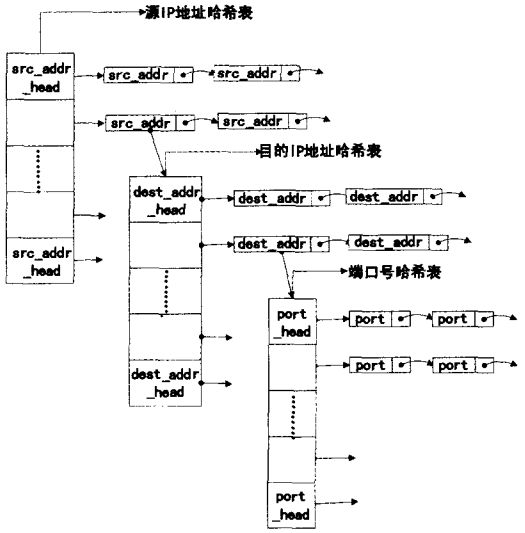

图3 网络连接哈希链表

4)计算目的端口的hash值，在dest_addr节点的port_head哈希链表中查对应目的端口的port链，在port链中查找是否有目的端口，如果有转到5，如果没有新建立一个port节点。

5)根据src_addr节点和dest_addr节点上存储的信息判断是否发生了扫描，即在一定的时间内，某一个机器是否访问了过多的目标ip地址，或目标端口，在src_addr和dest_addr上都保留有时间信息，访问的ip地址和端口数目信息，根据它们就可以计算出某一个机器访问过的目标ip地址数和目标端口数。

网络连接的状态是动态变化的，已经关闭的连接应该及时清除，否则会影响检测的准确性。系统采用定时清除和符合报警条件准备报警时清除相结合的方式，及时地把无效连接清除，保证了检测的准确性[8]。

4.2 基于协议分析的检测

基于协议分析的检测：由于采用了基于协议分析的检测方法大大加强了分析网络数据包的能力。协议分析有效利用了网络协议的层次性和相关协议的知识快速地判断攻击特征是否存在[9]。系统对大部分应用协议进行了完整彻底的分析，尽可能地缩减模式匹配的范围，可以直接对协议的关键部分进行检查，提高了协议分析的效率，它的高效使得匹配的计算量大幅度减小。

4.3 报警事件分类

传统的入侵检测系统对所有的攻击事件都会报警同时误报率也比较高，很容易导致事件风暴[10]。事件是IDS设备中对报警信息的称谓，报警信息通常都会显示在控制台上供管理员查阅，当产生大量报警信息时就会使管理员目不暇接，不能对所有的事件一一察看，从而可能会忽略一些重要的事件，这就是所谓的事件风暴。对于这个问题，系统对报警事件作了分类整理，将同一类别的报警信息归类成一条信息，减少了信息的数量，方便了管理员检查报警信息。同时这个分类功能是可供选择的，用户可以开启分类功能，也可以关闭它。

5 性能测试

系统在千兆环境下进行了测试，测试参数包括吞吐量、延迟等。

被测试的系统采用了四块X86 Node处理板，测试设备为SmartBits 6000B，测试软件为思博伦通信公司的应用代理专用测试软件TeraCaw。在加载一条安全策略和百条安全策略的情况下分别采用双向、120秒时间进行测试。系统在处理大包以及小包情况下都能达到千兆线速。各种情况下的吞吐量如表1所示。

表1 吞吐量测试结果

	占线速百分比	占线速百分比
帧长	一条策略	百条策略
64Byte	100%	100%
128Byte	100%	100%
256Byte	100%	100%
512Byte	100%	100%
1024Byte	100%	100%

运行SmartBits 6000B控制台的smartflow应用程序，选择latency进行设置，测试系统在700兆以及1000兆两种环境下三个不同帧长包的延迟，如表2所示。

表2 时延测试结果

帧长	占线速百分比	延迟(us)	占线速百分比	延迟(us)
64Byte	70%	3.2	100%	4.3
128Byte	70%	4.2	100%	4.9
256Byte	70%	5.1	100%	5.9

相对单一的采用网络处理器(NP)或专用集成电路(ASIC)技术实现的千兆入侵检测系统，在两种环境下的延迟都得到了很大的改善。

结束语 本文基于IXP2400、pp1200、TCAM芯片和CPCI 2.16技术开发了千兆线速入侵检测系统硬件平台，用硬件平台中的多个X86处理板对网络流量进行负载均衡，然后基于该平台设计并实现了一个千兆线速级入侵检测系统，解决了千兆网络环境中的入侵检测问题，并对系统实现中的部分关键问题进行了讨论。实验证明该系统比单一地采用网络处理器(NP)或专用集成电路(ASIC)技术实现的千兆入侵检测系统在性能和稳定性上有明显的优势，能够对千兆网络环境起到更好的保护作用。

参考文献

1 Mangione-Smith W H, Memik G. Network Processor Technologies. December 2001. http://www.cs.ucr.edu/~bhuyan/cs162/LECTURE8.ppt

2 Shrikumer H. 40Gbps de-layered silicon protocol engine for TCP record. European Design and Automation Association, 2006. 188～193

3 Small Packet Traffic Performance Optimization for 8255x and 8254x Ethernet Controllers. http://www.intel.com/design/network/applnots/ap453.pdf

4 Carr S, Sweany P. Automatic data partitioning for the agere payload plus network processor. Association for Computing Machinery, September 2004. 238～247

5 余荣，孙智. 高速网络入侵检测系统流量分配器. 清华大学学报-自然科学版，2005，45(10)

6 张军，苏璞春，冯登国. 基于系统调用的入侵检测系统设计与实现. 计算机应用，2006，26(9)：2137～2139

7 肖政宏，尹浩. 基于网络流量统计分析的入侵检测研究. 微电子学与计算机，2003，23(5)

8 刘利军，怀进鹏. 基于有穷自动机的网络扫描检测算法研究与实现. 计算机研究与发展，2006，43(3)：417～422

9 卜宏，黄皓. 一种应用层协议报文解析算法. 计算机应用研究，2003(2)

10 蒋建春，马恒太，等. 网络安全入侵检测：研究综述. 软件学报，2000，11(10)：1460～1467