高速网络环境下入侵检测系统结构研究

陈训逊 方滨兴 李 蕾
(哈尔滨工业大学计算机学院网络安全实验室 哈尔滨 150001)
(cxx@mail.nisac.gov.cn)

摘 要 提出了一种高速网络环境下的入侵检测系统体系结构,通过综合原始信号的耦合技术(捕包技术和流重组技术)、汇聚均衡技术以及高效的数据流引擎,有效地解决了在多线路、大带宽骨干网线路上进行网络安全分析的处理性能问题. 并且该体系结构具有很好的层次,具有高可伸缩性和适应性,可以适应从低速接入网到高速骨干网(oc48 以上多链路)的复杂网络环境和各种不同的接口形式. 当配置 16 个数据流总线时,能以线速处理八路 OC48 接口的网络数据,突破了公开报导的同类系统的最好水平.

关键词 入侵检测系统;高速网络环境;信号耦合;汇聚分流;散列;数据流总线;探针

中图法分类号 TP393.08

Architecture of Intrusion Detection for High-Speed Networks

CHEN Xun-Xun, FANG Bin-Xing, and LI lei
(*PACT Laboratory, College of Computer Science, Harbin Institute of Technology, Harbin* 150001)

Abstract The architecture of intrusion detection for high-speed networks environment is put forward. The architecture effectively solves the performance problems of network security analysis in multi-line and large bandwidth backbone networks by integrating raw signal capture (i.e. packets capture and stream reassemble), aggression and balance, and efficient data stream engine. The architecture has clear hierarchy, high scalability and flexibility and it can fit complex network environment and many types of interfaces from low speed access networks to high speed backbone networks (i.e. multi-OC48c lines). The ID system based on such architecture can achieve line-speed performance in eight-OC48c lines network environment when sixteen data streams are configured, which exceeds the best formally claimed performance report of nowadays ID systems.

Key words IDS; high-speed networks; signal coupling; aggressive-balancing hash; data stream; sensor

1 引 言

入侵检测系统(IDS)是目前解决网络安全问题的一个重要的和实用的技术手段. 随着网络规模的扩大、带宽的增长、技术的进步、用户数量的急剧暴涨,高速网络环境越来越多. 我们把高速网络环境定义为骨干网络中具有多条 2.5Gbps 以上速率线路的网络环境,IDS 一般部署在被保护网络的出口处和核心交换机上,当前 IDS 研究遇到的一个突出问题是数据处理速度受到极大的挑战. 著名信息安全研究和顾问机构 Gartner 公司提出论点,2005 年前 IDS 会逐渐消亡[1],其中 4 点理由中就有目前 IDS 对 600Mbps 以上的传输速率无力处理. 美国能源部将高速入侵检测系统作为 IDS 重点研究方向之一[2].

收稿日期:2003-07-15;修回日期:2003-10-17
基金项目:国家"八六三"高技术研究发展计划基金项目(2002AA147020)

到目前为止,国际上公开发表的相关成果较少,Sekar 等人提出了一个可以到 500Mbps 处理速度的高性能 IDS[3],但它是基于离线数据的;IIS 的 Giga Sentry 和 Cisco 的相关产品可以达到 50Kpps 的处理速度. 较实用的高速入侵检测系统体系结构是 Christopher Kruegel 等人提出的高速网络有状态入侵检测系统结构[4]. 该系统由一个网络数据捕获器(network tap)、一个流量分发器(traffic scatterer)、一组(m 个)流量转发器(traffic slicers) $S_0,\cdots,S_{m-1}$、一个交换机(switch)、一组(n 个)数据流重组器(stream reassemblers) $R_0,\cdots,R_{n-1}$ 以及一组(p 个)入侵检测探针(intrusion detection sensors)等 6 个部分组成. Tap 用来获取一定时间段 Δ 中原始的高速带宽网络数据帧序列 $F=\langle f_0,f_1,\cdots,f_t\rangle$ 传送给流量分发器,分发器按照某种分类算法将 F 分流成 m 个子序列 $F_j:0\leqslant j<m$. 每个 F_j 是 F 的一个子集(可能为空集). 每个数据帧 f_i 是属于并且仅属于某个子序列 F_j 的一个元素,因此有 $\bigcup_{j=0}^{j<m}F_j=F$. 分类算法采用 round-robin 算法将 F 平均分流成 m 个子序列,因此每个 F_j 包含总流量的 m 分之一. 每一个子序列 F_j 发送到一个流量转发器 S_j,转发器的作用是将 F_j 中相关联的数据帧(属于用一个攻击场景中的各个数据帧)转发到相同的重组器上. m 个转发器和 n 个重组器通过交换机互连到一起,形成 $m\times n$ 的单向交叉矩阵. 原始大流量通过分散和重定向变成若干单个探针可以处理的小流量,从而既解决了流量问题,又避免了信息缺失.

该体系结构有效地解决了大流量环境下的流量分流问题,使得后端的处理系统可以按集群的形式处理远远超过单结点处理机的数据,并且可扩展性很强. 但是该结构存在着两个不足之处:一是该结构只针对单条大流量线路进行监测,需要对多线路(大多数情况)监测体系结构进行扩展;二是入侵检测探针之间需要有通信通道进行协同工作以分析多线路情况下的关联时间. 我们对上述两点进行了补充,并对流量分发器、转发器和交换机进行了合并,形成了一个复杂多线路大流量网络环境下的入侵检测体系结构,如图 1 所示:

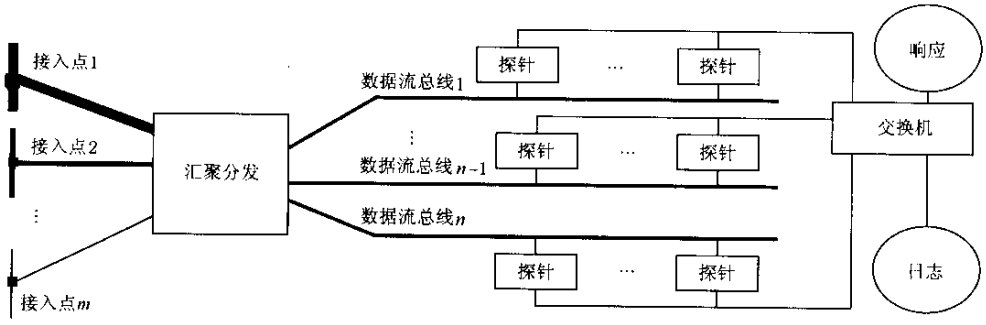

图 1 高速网络环境入侵检测系统结构

该体系结构由一组(m 个)原始信号耦合器、汇聚与分流子系统、一组(n 个)数据流总线、探针(n 组)、响应机制(可选)和日志子系统组成. 下面分别对这几个子系统的功能和结构进行描述.

2 原始信号耦合器

原始信号耦合器指网络原始数据输出机构,例如交换机的镜像端口、HUB 的监听端口等. 通过这些端口将线路上的数据信号完整地复制出来,送到下一级进行初级处理. 随着网络技术和传输技术的发展,原始信号源的单线带宽经历了十兆级(以太网、E1、E3 等接口)、百兆级(FE,OC-3,OC-12 等接口)、千兆级(GE,OC48 等接口)带宽以及目前的万兆级(10GE,OC192 等接口)带宽. 目前,由于各个运营商发展的不平衡和不同应用环境的需要,在国内企业网和运营商网络中同时存在上述原始数据接口形式.

原始信号的耦合技术是基于侦听机制的,目前的侦听机制有 4 种:共享 HUB 侦听、设备端口镜像侦听、部分种类接口的光耦合侦听以及专用设备侦听. 如果线路中没有以上设备/线路的环境下,需要做传输协议转换. 具体对应如下的原始信号耦合技术:

(1) FE/Ethernet 线路(电口)信号耦合技术

该技术适用于电接口的以太网(Ethernet)、快

速以太网(fast Ethernet)线路的数据获取. 优点是双向数据同时获取减少了汇聚环节,缺点是在双向流量之和接近或超过单条线路带宽时会造成监听线路拥塞,对于共享 HUB 来说还会由于冲突的增加导致线路可利用带宽的急剧下降,对于镜像端口则可以通过增加镜像端口数量来提高侦听能力, 但需要采用汇聚技术. 解决方法是使用高带宽端口做侦听端口,例如使用 GE 端口做 FE 端口的侦听,以避免拥塞的出现(如图 2 所示).

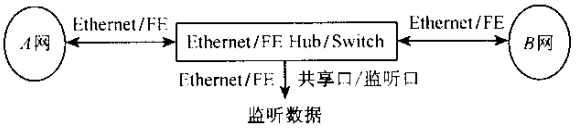

图 2　FE/Ethernet 线路(电口)信号耦合技术

(2) 低速 WAN 线路信号耦合技术

图 3 中的转换设备可以是 3 层设备也可以是链路层设备,如果采用 3 层设备则需要在上面进行路由的配置,但是可以用于多路 WAN 汇聚转换,适用范围广;如果采用链路层设备则不需要 3 层配置,只需进行简单的安装配置即可,但是只能用于单路转换,并且不支持 WAN 汇聚. 该技术适用于 DDN, E1,E3 等广域网线路的信号耦合(如图 3 所示).

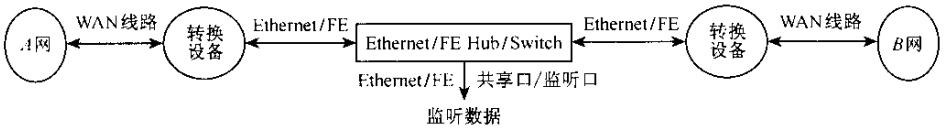

图 3　低速 WAN 线路信号耦合技术

(3) 光纤链路信号耦合技术

该种技术在有线电视信号传输和计费系统中应用较多,采用光耦合器件可以将光信号复制出一份或多份,特点是无源设备,运行稳定,但是双向数据分别输出,需要汇聚,而且不能进行无用数据过滤. 适用于 GE, 10/100BASE-FX 等光接口(如图 4 所示).

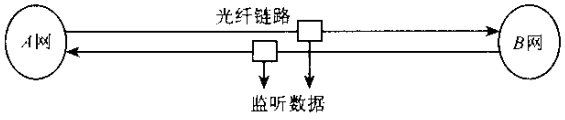

图 4　光纤链路信号耦合技术

(4) 专用信号耦合设备

专用数据获取设备可以在输出监听数据之前对数据做一定的预处理,例如滤除无效包、攻击包等. 特点是串接在线路中,可能对原始数据信号有损,对其可靠性和容错能力有较高要求. 该技术在通信仪表中应用较多(如图 5 所示).

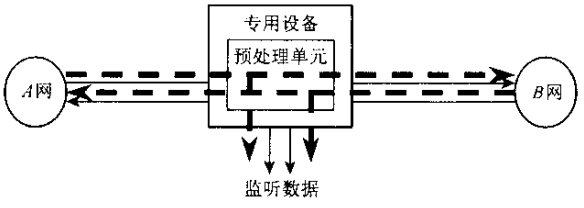

图 5　专用信号耦合设备

3　汇聚与分流子系统

负责将原始网络数据流进行必要的接口转换——将网络设备通信接口(如 Pos, ATM, E1 等)转换成主机通信接口(如 FE, GE 等),并且进行数据的合并和均衡分流后输出到处理机群上. 在低带宽的网络环境下,如果监听数据的输出端口为主机接口形式(如 FE, GE 等)则可以通过在探针设备上配置多块接口卡来接收原始数据信号,直接处理. 如果被保护网络和外部网络之间存在多条线路,则有多条监测数据线路,需要对这些线路汇聚后再按流分类后均衡输出到数据流总线上.

(1) 交换设备汇聚技术

该技术适用于 FE/GE 监测线路,为每个监测线路接收端口分配一个单独的 VLAN,配置高速汇聚端口(GE),通过 SPAN 将所有监测线路接收端口进入的流量镜像到汇聚端口上输出. 这样某一路监测数据进入汇聚交换机后就被复制一份到汇聚端口输出.而对于进入的原始包,交换机由于找不到包中目的 MAC 地址对应的输出端口,并且该路监测数据接收端口所在 VLAN 中也没有其他活动端口可供广播,这样交换机会将原始包丢弃,不会产生干扰.该技术适用于监测线路流量之和小于包处理机能处理带宽的环境(如图 6 所示).

(2) 基于散列流分类的汇聚均衡技术

当监测线路流量之和超过单台包处理机能处理

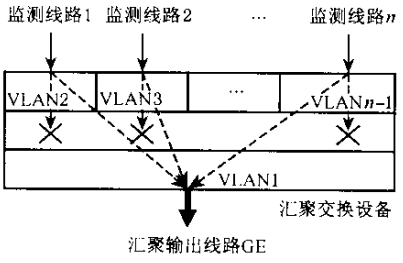

图 6 交换设备汇聚技术

的带宽时,需要进行分流,为了达到一定的均匀度,分流算法必须具有足够细的粒度. 目前有两种选择,一种是按照目的 IP 地址进行分流,优点是采用通用配置的路由设备即可达到目的,缺点是输出流量变化幅度较大,流量变化曲线上有尖锐毛刺,均方差不理想,在恶劣条件有可能超过输出端口带宽或包处理机处理能力,从而造成丢包或包处理机拥塞. IP 地址分流很难做到各个输出端口流量均匀,但是除去突发流量外,大多数时间输出流量比较稳定. 因此该技术在流量负载不是很重的网络环境下仍然是一种经济的选择. 另一种是按照流进行分流(原始技术源自 4-7 层交换机和 4-7 层负载均衡系统如图 7 所示),即对数据包 p 中和流相关的若干参数(源地址 Sip,目的地址 Dip,源端口 Sp,目的端口 Dp)进行某种散列运算 $H(Sip,Dip,Sp,Dp)$,$H(p)$ 满足如下条件:

$$H(Sip,Dip,Sp,Dp) = H(Dip,Sip,Dp,Sp).$$

设有 n 个输出端口,对于一个到达的数据包 p,输出端口号 Tn 的计算如下:

$$Tn = H(Sip,Dip,Sp,Dp) \bmod n + 1.$$

$H(p)/n$ 越大则分流粒度越小,分流越均匀,抗流量尖峰脉冲的能力越强,这是由于对于出现集中 IP 地址相关的大流量数据时(如大型网站访问流量、高速代理服务器等),TCP 流的目的地址虽然不变,但源端口是不断变化的(对于大多数客户机来说是循环递增的). 目前很多新型的通用 3 层设备上支持的流分类功能也可以基本完成按流进行分流的

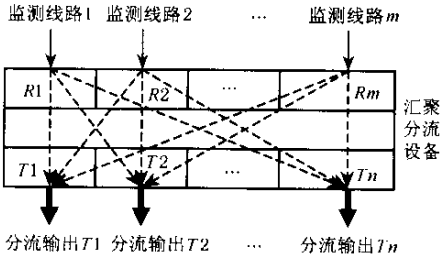

图 7 基于散列流分类的汇聚均衡技术

功能. 上述两种分流技术的实验对比数据如图 8、图 9 所示.

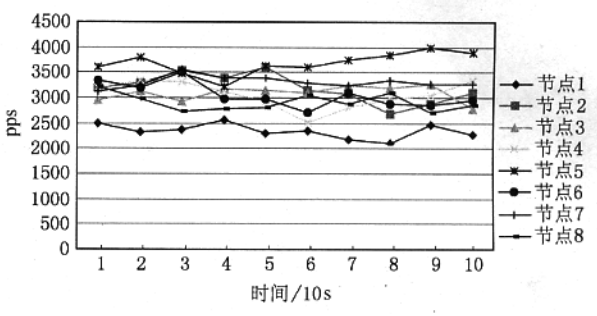

图 8 基于散列流分类的分流效果

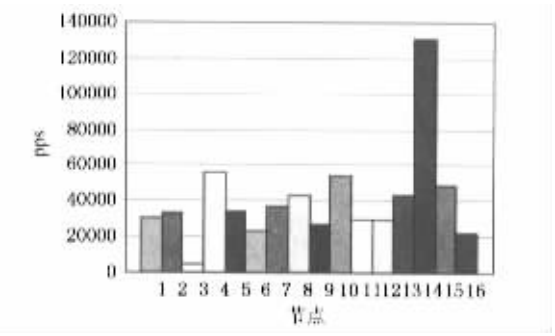

图 9 基于 IP 地址的分流效果

4 数据流总线

由于探针对原始网络数据需要进行还原、解码、匹配反复查找等操作,是很消耗 CPU 资源的. 因此需要多个完成不同功能的专用探针来对一份原始数据进行加工,而在大带宽的高速网络环境下,对原始网络数据先存储再处理是不现实的,所以需要一个总线系统来对所有的探针进行原始数据广播. 针对目前常见的主机接口 FE 和 GE,分别有快速以太网总线和光耦合两种常用形式. 快速以太网总线是通过 HUB 设备将各个探针和分流子系统的输出端口连接起来,将探针的接收端口置为静默模式,从而实现一到多的数据链路层的数据复制功能,特点是通过信号再生放大,能量不减少,但错误包会被丢弃. 光耦合方式是采用光耦合器进行物理层的信号无源复制,特点是不会丢失任何异常包,但是能量会下降,因此可以挂接的探针数目受到限制.

5 探 针

IDS 探针完成数据包的接收、数据流还原、解码、攻击特征的分析等功能,有状态的探针还需要保持每个连接的状态. 探针软件主要由数据流引擎和

分析引擎构成.

5.1 数据流引擎

数据流引擎的功能由 2 部分组成:第 1 部分完成接收原始数据整形器传送来的数据包,放入用户缓冲区中的功能,一般称为捕包技术;第 2 部分是流重组,完成数据帧→IP 分片→IP 报文→TCP 层连接的逐级重组功能.

捕包技术的发展到目前为止经历了 3 个阶段:第 1 阶段是利用操作系统提供的库函数进行捕包,例如 Linux 中的 libpcap 库、Windows 中的 Winsock2 库等,特点是硬件兼容性好、操作系统兼容性好. 但是由于数据包从到达网卡、通过 DMA 到内核存储空间再经过若干次拷贝到达用户空间开销较大,很难达到很高的捕包速率(2GHzCPU 的主机 Linux 可达到 50 Kpps 的捕包速率,FreeBSD 性能会更高一些)并且由于某些操作系统(如 Linux)采用每到一个包产生一次中断的方式,所以当包流量过大时系统会因为中断过于频繁而陷入瘫痪.

第 2 阶段是采用一些缓冲技术,例如修改网卡参数降低中断频率,编写专用驱动程序在数据包到达核心内存空间后进行缓冲,积累一定数量后(如 1K 个数据包)提交给用户应用程序. 此种模式的硬件兼容性仍然较好,但和操作系统耦合性较强性能相比,第 1 阶段有较大提高(2GHzCPU 的主机 Linux 操作系统下可达到 100 Kpps 以上的捕包率).

第 3 阶段是采用零拷贝技术,修改网卡驱动程序,使得网卡在收到一定数量的包后直接通过 DMA 将数据包传送到用户内存空间的缓冲区中,将捕包功能内存拷贝的次数降为 0(零拷贝因此命名). 此种模式的硬件透明性较差,必须详细了解网卡的技术资料,并且由于捕包操作跨过了系统协议栈,因此和操作系统的耦合性较强,但是由于解决了捕包中的内存拷贝等瓶颈,使得性能有大幅提高(2GHzCPU 的主机 Linux 操作系统下可达到 600 Kpps 以上的捕包率,在混合包长下可以很容易做到真正的千兆线速捕包,从而使千兆接口的防火墙真正的实用).

流重组技术基本是依据 TCP 协议栈的相关标准,采用有限状态自动机(FSA)的技术进行还原. 由于有很多的技术专门针对 IDS 的流重组进行破坏,如Mark Handley 等人提出的插入攻击和逃避攻击以及连接池 DoS 等[5],因此,在重组时需要考虑对应的识别方法. 一般可以采用异常检测(如 Mahoney等人提出的 PHAD[6])、流量整形[4]的方法.

5.2 分析引擎

分析引擎的功能是将传输层中承载的数据进行会话恢复、高层协议还原、解码、解压缩和代码转换等工作形成状态化信息流,然后使用已经构造好的敏感信息模式对信息流进行匹配,对匹配成功的流记录日志并通知响应机制. 分析引擎所做的工作都是 CPU 密集型的工作,是占用 CPU 资源最多的一个部件. 它的性能和效率决定了信息入侵检测系统的处理能力. 从功能上,分析引擎分为两个模块,一个是协议分析模块,负责还原数据流中各种感兴趣的应用层协议,对信息流进行结构分析,生成各类结构化信息流. 另一个模块是模式匹配机,根据已知的敏感模式库对结构化信息流中每一个感兴趣的结构进行模式匹配,寻找敏感模式.

协议分析模块还原数据流中指定的应用层协议,如 HTTP,SMTP,POP3,BBS 等,保存每个流应用层协议的状态,还原出可以进行内容匹配的数据流,如 HTTP 中需要分割出 HTTP 中各个头字段(URL,HOST,CONTENT-TYPE 等),需要识别出 HTTP BODY 中传输的内容类型和起始分界,再如 SMTP 中需要还原出发信人、收信人、主题、信体、附件等内容,并需要进行解码、边界识别和嵌套信体识别等工作.

为了提高效率,对于敏感关键字的匹配采用有限状态自动机(FSA)进行字符串匹配[7,8]. 由于需要对输入的每一个信息结构进行匹配,因此需要采取空间换时间的策略,使用多模式有限状态自动机(MP-FSA),对输入信息流进行一次性关键字匹配,对于需要模糊匹配的模式也要对匹配模式进行扩展,采用多模式扩展有限状态自动机(MP-EFSA)进行匹配.

对于非关键字匹配类的模式匹配则需要单独处理,即同一个结构多次处理. 要求非关键字匹配类的模式匹配一定是轻量级的(light-weight).

6 响应机制

响应机制又称为联动机制,也是 IDS 领域的热点研究方向之一,它的功能是实时地阻断攻击流在被保护网络和外部网络之间的连接,以主动终止攻击的过程,它是入侵检测系统的主动执行机构. 由于响应机制很容易被攻击者利用,或者引起自身的失效,或者充当了 DDOS 的跳板机,因此一直以来学术界建议一般情况下不要启动 IDS 的响应机制.

但是,由于攻击手段越来越丰富,往往在很短的时间内对网络产生致命的影响,而给人判断和处理的时间越来越少. 所以,如何有效地对攻击行为进行实时响应,以及和网关设备、主机设备的联动是一个意义重大的研究课题.

响应机制的发展已经经历了 IP 包过滤(静态 IP 包过滤、动态 IP 包过滤)、连接欺骗(传输层连接欺骗、应用层连接欺骗)两个阶段,并且形成了针对不同的应用多种方式共存的现状. 目前正在向第 3 阶段——实时连接过滤发展.

静态 IP 包过滤是 IDS 通过和被保护网络与外部网络之间的连通边的端点网络层设备(路由器、三层交换机等)进行联动,在其上设置访问控制列表(access control list,ACL)或静态路由表来实现对指定 IP 地址的过滤[8]. 由于需要过滤的 IP 地址数量很大,大多数的网络层设备上对 ACL 大小和性能的支持不能满足要求,因此,实际工作中大多采用静态路由的方式. 使用该种方式,信息入侵检测系统只能通过专用客户端程序静态写入的方式进行访问控制,粒度大(IP 地址级),响应时间较慢,容量较小,但是可以静态写入路由设备的配置文件中,是非易失的.

动态 IP 包过滤[8]是指入侵检测系统采用动态路由协议(BGP,OSPF 等)和关键路由设备进行路由扩散,将需要过滤的 IP 地址扩散到路由设备中的路由表中,特点是响应时间快、容量大,但是只能动态地写入路由设备内存(RAM)中的路由表中,是易失的,同样粒度大. 连接欺骗指信息入侵检测系统在敏感连接传输过程中伪造连接结束信令(RST,FIN)发送给连接的源和目的地址,以中断该连接. 特点是实时强、粒度小(连接级),可以针对某一次敏感连接进行阻断. 缺点是对分析系统工作状态依赖较强,需要向业务网上发送数据包,易受 DoS 攻击.

通过和连接级防火墙设备进行联动,可以针对连接五元组(传输协议类型、源地址、源端口、目的地址、目的端口)对数据流进行过滤. 可以针对指定的任意五元以内的组合条件进行过滤,实时性强、粒度小.

7 日志机制

对于一个 IDS 来说,为了和人沟通、报警的需要,日志机制是必不可少的一个关键部件[9]. 对于高速网络环境下的 IDS 来说,日志机制的性能至关重要. 由于 IDS 是一个警报系统,因此除了确定已知的攻击行为外,IDS 还将生成一定数量的异常行为报告信息,而这些信息在一个高速网络环境下生成的速度往往远远超过人的处理能力,重要的攻击报警信息会被淹没在大量无用的报警信息之中,从而逃过检查[10,11]. 所以,在高速网络环境下的 IDS 中,日志机制必须重新设计,需要进行报警信息的多次处理,进行数据融合、聚类和分类[12~14],以使重要的信息突出,一般性的信息隐藏. 国际上对该方向的研究有了一些成果,在这方面也已经有产品出现,但是数据融合的方法还显简单,效果不是十分明显[15],仍然有相当长的路要走.

8 总 结

本文提出的高速网络环境下的入侵检测系统体系结构有效地解决了在多线路、大带宽骨干网线路上进行网络安全分析的处理性能问题. 并且该体系结构具有很好的层次,具有高可伸缩性和适应性,可以适应从低速接入网到高速骨干网的复杂网络环境和各种不同的接口形式. 通过骨干网实验,配置 16 个数据流总线即可以线速处理八路 OC48 接口网络数据.

参 考 文 献

1 A Haines. Gartner Information Security Hype Cycle Declares Intrusion Detection a Market Failure. http://www3.gartner.com/5_about/press_releases/pr11june2003c.jsp.2003

2 J Allen, A Christie, W Fithen, *et al*. State of the practice of intrusion detection technologies. Software Engineering Institute, Carnegie Mellon University, Tech Rep: CMU/SEI-99-TR-028, 2000

3 R Sekar, Y Guang, S Verma, *et al*. A high-performance network intrusion detection system. The 6th ACM Conf on Computer and Communications Security, New York, 1999

4 C Kruegel, F Valeur, G Vigna, *et al*. Stateful intrusion detection for high-speed networks. In: Proc of the IEEE Symposium Security and Privacy. Los Alamitos, CA: IEEE Computer Society Press, 2002

5 M Handley, V Paxson, C Kreibich. Network intrusion detection: Evasion, traffic normalization, and end-to-end protocol semantics. The USENIX Security Symposium, Washington, DC, 2001

6 M V Mahoney, P K Chan. PHAD: Packet header anomaly detection for identifying hostile network traffic. Department of Computer Sciences, Florida Institute of Technology, Tech Rep: 2001-04, 2001

7 R Bettati, W Zhao, D Teodor. Real-time intrusion detection and suppression. The 1st USENIX Workshop on Intrusion Detection and Network Monitoring, Santa Clara, CA, 1999

8　李蕾,乔佩利,陈训逊. 一种 IP 访问控制方法的设计和实现. 信息技术,2001,(5): 38～38
(Li Lei, Qiao Peili, Chen Xunxun. An IP access controlling method—Design and implementation. Information Technology(in Chinese), 2001, (5): 35～38)

9　Dorothy E Denning. An intrusion—Detection Model. IEEE Trans on Software Engineering, 1987, SE-13(2): 222～232

10　K Das. The development of stealthy attacks to evaluate intrusion detection systems:[Master dissertation]. Cambridge, MA: MIT Department of Electrical Engineering and Computer Science, 2000

11　D Song, G Shaffer, M Undy. Nidsbench—A Network intrusion detection system test suite. The 2nd Int'l Workshop on Recent Advances in Intrusion Detection (RAID), West Lafayette, Indiana, 1999

12　W Lee, S Stolfo. Data mining approaches for intrusion detection. The 7th USENIX Security Symposium (SECURITY-98), San Antonio, Texas, 1998

13　W W Cohen. Fast effective rule induction. In: Proc of the 12th Int'l Conf on Machine Learning (ICML-95). San Mateo, CA: Morgan Kaufman, 1995. 115～123

14　V Paxson. Bro: A system for detecting network intruders in real-time. The 7th USENIX Security Symposium, San Antonio, TX, 1998

15　R Lippmann, J W Haines, D J Fried, *et al*. The 1999 DARPA off-line intrusion detection evaluation. Computer Networks, 2000, 34(4): 579～595

陈训逊　男,1972 年生,博士研究生,主要研究方向为计算机网络、信息安全,曾获 2002 年国家科技进步一等奖.

方滨兴　男,1960 年生,教授,博士生导师,主要研究方向为计算机网络、信息安全,曾获 2002 年国家科技进步一等奖(bxfang@mail.cnnisc.gov.cn).

李　蕾　女,1972 年生,博士研究生,主要研究方向为计算机网络、信息安全(lilei@pact518.hit.edu.cn).

高速网络环境下入侵检测系统结构研究

作者： 陈训逊， 方滨兴， 李蕾
作者单位： 哈尔滨工业大学计算机学院网络安全实验室,哈尔滨,150001
刊名： 计算机研究与发展 ISTIC EI PKU
英文刊名： JOURNAL OF COMPUTER RESEARCH AND DEVELOPMENT
年，卷(期)： 2004,41(9)
被引用次数： 9次

参考文献(15条)

1. R Sekar;Y Guang;S Verma A high-performance network intrusion detection system 1999

2. J Allen;A Christie;W Fithen State of the practice of intrusion detection technologies. Software Engineering Institute, Carnegie Mellon University 2000

3. A Haines Gartner Information Security Hype Cycle Declares Intrusion Detection a Market Failure 2003

4. R Lippmann;J W Haines;D J Fried The 1999 DARPA off-line intrusion detection evaluation[外文期刊] 2000(04)

5. V Paxson Bro: A system for detecting network intruders in real-time 1998

6. W W Cohen Fast effective rule induction 1995

7. W Lee;S Stolfo Data mining approaches for intrusion detection. The 7th USENIX Security Symposium (SECURITY-98) 1998

8. D Song;G Shaffer;M Undy Nidsbench-A Network intrusion detection system test suite 1999

9. K Das Th dvpmnt f stathy attacks t vauat intrusin dtctin systms 2000

10. Dorothy E Denning An intrusion-Detection Model 1987(02)

11. 李蕾;乔佩利;陈训逊 一种IP访问控制方法的设计和实现 2001(05)

12. R Bettati;W Zhao;D Teodor Real-time intrusion detection and suppression 1999

13. M V Mahoney;P K Chan PHAD: Packet header anomaly detection for identifying hostile network traffic. Department of Computer Sciences, Florida Institute of Technology 2001

14. M Handley;V Paxson;C Kreibich Network intrusion detection: Evasion, traffic normalization, and end-to-end protocol semantics[外文会议] 2001

15. C Kruegel;F Valeur;G Vigna Stateful intrusion detection for high-speed networks. In 2002

引证文献(9条)

1. 曾峰. 祁邨邨 高速网络环境下入侵检测技术探讨[期刊论文]-福建电脑 2010(7)

2. 石飞. 史岚. 乔建忠. 莫晓静 网络数据采集技术研究[期刊论文]-小型微型计算机系统 2008(10)

3. 石飞. 史岚. 乔建忠. 莫晓静 网络数据采集技术研究[期刊论文]-小型微型计算机系统 2008(10)

4. 陈一骄. LU Xi-Cheng. 时向泉. SUN Zhi-Gang 一种面向会话的自适应负载均衡算法[期刊论文]-软件学报 2008(7)

5. 陈一骄. LU Xi-Cheng. 时向泉. SUN Zhi-Gang 一种面向会话的自适应负载均衡算法[期刊论文]-软件学报 2008(7)

6. 叶进星. 翟伟斌. 刘宝旭. 蒋卓明. 许榕生 基于MPMF算法的高速网络内容审计系统架构[期刊论文]-计算机工程 2007(14)

7. 张新刚. 刘妍. 王星辉 基于入侵检测系统(IDS)的分析与研究[期刊论文]-网络安全技术与应用 2006(6)

8. 李浪. 李仁发. 李肯立. 许琼方 一种高速网络下分布式入侵检测体系结构的设计与实现[期刊论文]-衡阳师范学院

学报 2006(3)

9. 王文奇 入侵检测与安全防御协同控制研究[学位论文]博士 2006