ISSN1000-9825 Journal of Software 软件学报 2000,11(5):642~645

一个基于 Agent 的防火墙系统的设计与实现*

张磊 卿斯汉

(中国科学院软件研究所 北京 100080)

(中国科学院信息安全技术工程研究中心 北京 100080)

E-mail: {zhang,qing}@ercist.iscas.ac.cn

摘要 分析了现有的防火墙系统及其弱点.在此基础上,引入了"Agent"的概念.应用"Agent"的定义和方法来规范防火墙的各个部件,描述了各"Agent"之间的通信和协作,并说明了设计和实现一个基于"Agent"的防火墙系统的方法和过程.

关键词 防火墙,Agent,IP 包过滤,应用代理,安全审计.

中图法分类号 TP393

随着计算机网络,特别是近年来 Internet 的飞速发展,各公司、企业、政府机关交流信息的方式也在发生变化.但这些部门面临的最大问题就是,如何用一种有效的企业安全解决方案来保护网络及信息系统不受内部的和外部的恶意攻击.在众多方案中,防火墙是企业安全解决策略的关键部分.传统的防火墙一般放在一个企业与公网互连的入口处.在安全策略上,认为网络内部是一个单一而可信的实体,主要是防护来自 Internet 的网络"黑客"的攻击,以保护内部网络的信息和资源的安全.然而,一个企业的内部结构和各部门对安全的要求一般是多样和复杂的,而且一个统一的、完善的安全策略也不容易制定.所以,一般需要分布在不同节点上的多个防火墙协同工作.另外,为了方便管理,对于一个企业内部网络(Intranet)中所有的防火墙要能进行远程控制.这样,就要求防火墙系统,在功能上能支持各种不同的网络服务;在结构上要具有可适应性、可伸缩性;在管理上要能够动态监控、动态配置、实时报警,并且分布式的防火墙之间能进行标准通信,协调工作.

基于对防火墙的这种要求,我们在设计上引入"Agent"的概念和方法[1~4],用"Agent"定义来规范防火墙中各个部件的需求和实现,利用"Agent"之间的通信,实现各部件之间的通信.本文的研究重点是防火墙系统内部各部件的设计、实现以及各部件之间的协调.

1 基于 Agent 的模型

我们的系统是基于 Agent 模型的.在系统中,一个应用由一系列互连着的部件构成.这些部件就是可以对事件(event)作出反应(reaction)的"Agent".将这样的 Agent 加入到分类部件模型中,就允许应用的设计者通过对分布式的应用能很容易地添加新的功能而无需改变它的其他主要部件.构成一个应用的部件和 Agent 可能分布在不同的站点(网络节点)上,这样可以将一个应用的任务分布式地执行,可以解决防火墙通常产生的网络瓶颈问题并增强网络的可靠性.

所有 Agent 的活动是根据一个基于事件的运行模型来进行的.一个事件被一个 Agent 接收后,触发一个反应,并且它自己也可能发出一个新的事件.一个完整的执行过程是:{事件接收—反应—事件发出}.

我们的防火墙系统是一个安全系统,它被放在两个网络的连接处,用来过滤两个网络之间的信息交换.下面,对它的操作进行简单的描述:每一个通过防火墙的 IP 包都会被检查和分析.基于这种分析,IP 包或者被转

* 本文研究得到国家自然科学基金(No.69673016)资助.作者张磊,1968 年生,博士生,主要研究领域为网络信息安全,防火墙技术.卿斯汉,1939 年生,研究员,博士生导师,主要研究领域为信息安全理论和技术.

本文通讯联系人:卿斯汉,北京 100080,中国科学院软件研究所

本文 1999-02-05 收到原稿,1999-07-07 收到修改稿

发,或者被丢弃,并且将必要的数据记录审计.另外,对于应用层的各种服务,防火墙作为内外通信的代理(proxy),所有对这种服务的访问都是先与代理建立连接,再由代理与目的服务器进行连接.在代理过程中,由代理根据设定的安全控制规则,或者转发访问,或者阻断.这样就实现了对应用服务的控制.所有执行访问控制规则都是由管理员事先制定好的.这些规则可能定义在OSI网络层次结构的各个层次上,可能是对IP层的IP包进行控制,也可能是对应用层的各个应用服务进行控制.

图1展示了单一防火墙的总体结构.本文的主要目标是使防火墙的结构更加灵活,允许应用分布到不同的网络节点上执行,允许应用能够被动态地重配置(根据用户的要求会增加新功能),并且这个工作是在用户层完成的,无需修改系统内核,这就使得在Agent的概念基础上来构造用户层的子系统.这样,增加新功能或对现有的系统按用户的特殊要求进行构造就可以通过增加或删除Agent或改变Agent之间或与其他部件之间的互连模型来实现.

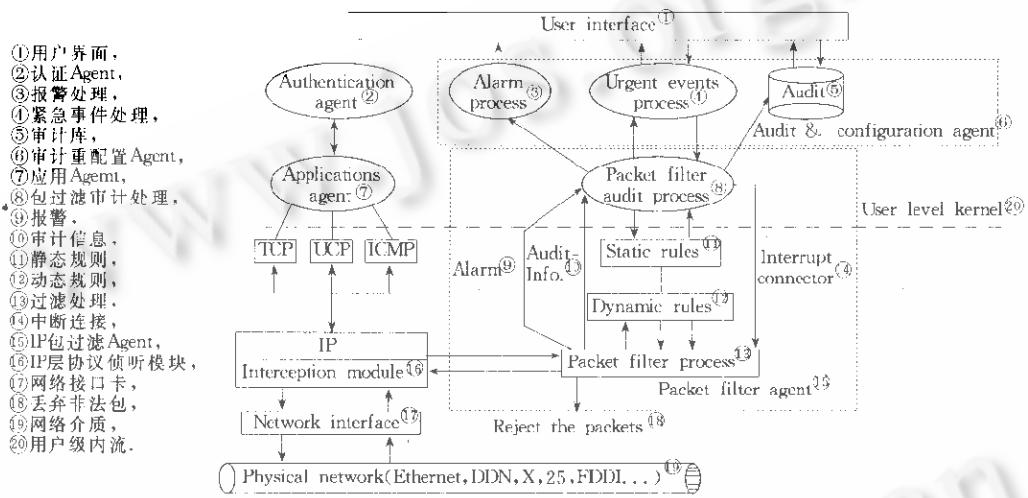

Fig.1. The architecture of firewall
图1 防火墙总体结构图

2 Agent部件实现

根据上述基于Agent的模型,系统从功能上来看,可分为以下4类Agent(如图1所示).

2.1 IP包过滤Agent

IP包过滤是最早的、也是最简单的防火墙系统.在我们的系统中,也采用传统的物理配置,在一台Sun Ultra10 Solaris 2.5上安装两块网卡,并将内外网络分别接在不同的网卡上.这样,内部网络与外部网络在两块网卡之间隔离开来.当有信息(IP包)要进出网络时,检查进出网络的规则(ACL)表,如果是合法包,就将此IP包转发到另外的网卡上发送出去,这样就使得一个IP包成功地进(出)了网络;否则,将IP包丢弃,阻断了进出网络的连接.为了获得所有要进出网络的IP包,在标准内核中插入一个侦听模块.通过它,可以截取所有进出主机的数据帧.然后,分析出IP包,再对IP包进行安全策略检查.同时,对通信进行审计或报警.

在对IP包进行过滤的处理过程中,我们采用了近年才出现的动态过滤和有状态的过滤技术[5],它不仅可以克服传统的简单过滤的方法所存在的弱点,而且结合审计处理,可以对网络入侵进行实时处理.

传统的包过滤不考虑TCP协议的连接状态,所以在设置规则时,就要预先设置能包容所有允许应用的允许条件.这样,"入侵者"就可假冒被允许的TCP连接,对网络进行攻击.我们仔细分析了TCP/IP协议和各服务协议,首先设定尽可能小的允许通过规则,在进行IP包转发时,通过监控TCP连接的状态,动态地生成一些规则,就可达到既能使合法IP包正常通过,又能防止非法入侵的目的.对包过滤的审计和报警是由包过滤审计处理模块来完成的,它可以与审计和重定义Agent进行通信,再由审计Agent通知用户;它还能得到阻断网络通信的命

令,修改动态规则设置,快速截断网络,以实现对网络入侵的及时处理.

2.2 应用服务 Agent

它主要代理进出网络的应用层服务,使各项请求顺利通过网关安全策略的检查.它也能记录和跟踪可疑IP或可疑用户的操作,并发出报警信息.

我们的系统是建立在现有的代理防火墙之上的.系统由多个代理服务程序组成.对常见的应用(如Telnet,FTP,HTTP,...)都有相应的代理,对于一些新出现的应用服务和其他未开发的服务,则提供了一个通用代理.

为了扩充认证方式和增加结构的适应性,我们将代理中有关认证的部分抽取出来,用一个统一的认证接口来完成与认证 Agent 的通信,并且认证协议和过程与代理无关,它只是在开始和结束认证时,与认证处理模块交换信息.

应用服务 Agent 中也有审计,它主要接收各种代理模块发来的审计和报警信息,经过分析处理后,将它们送给审计和重定义 Agent,并通过它,向用户报警.

2.3 认证 Agent

认证 Agent 的主要功能就是提供多种认证方案,以支持多种用户认证请求.通过与应用服务 Agent 的通信,可接收认证请求,并能返回用户的授权信息.

在一个认证系统中,如果有多种认证方案可以由管理员选择,则可针对不同类型的网络用户,制定不同的认证方案.例如,对内部网络用户可以只用明文的方式进行认证,而对于外部用户,则必须采用S/Key(1次1密)和MD5(C/R)等较强的身份来认证.所以,为了使防火墙系统的应用范围和领域更广泛,应该使认证方案具有灵活性和可扩充性.

2.4 审计重配置 Agent

一般来说,一个完美的安全网络系统不仅具有保护能力,而且还应该具有检查出异常状态的能力.同时,允许系统管理员分析可疑事件的原因.在我们的系统中,提供了在IP层和应用层发生的可疑事件的详细记录.它们可以帮助管理员通过对审计结果的详细分析,而对系统的安全策略重新评价和重定义,使系统逐渐健壮.

审计和重定义 Agent 的功能主要是接收其他 Agent 发来的报警信息,作出相应的反应(如向用户报警),并能通过对可疑信息的分析,人工干预或自学习地对系统进行安全策略的重新配置.此外,它还可以在紧急情况下,向IP包过滤 Agent 和应用服务 Agent 发出强制中断的命令,以达到实时处理意外事件、保护网络和资源的目的.

3 通信环境

在多 Agent 系统中,Agent 之间的交互在很大程度上是通过"通信"实现的[6].在我们的运行环境中,我们采用了一个"Message queues"来作为 Agent 的通信基础.其通信内容为一个四元组,即

〈通信内容〉::=〈发送者〉〈接收者〉〈时间〉〈数据流〉.

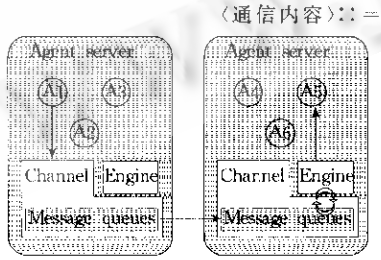

Fig. 2 The internal structure of message queues
图2 Message queue的内部结构

从程序设计的层次来看,Agent 之间的通信是由事件刺激执行的.当一个事件发生时,一个 Agent 就会向消息队列中发送一个消息;消息队列接收到消息,就会根据消息的目的地进行转发;当目的消息队列接收到新消息时,则利用Engine激活接收 Agent 接收消息,并执行任务.在这个过程中,事件是 Agent 之间通信、同步和共享信息的唯一途径.通信机制基于消息排队的性质,它是异步的、可靠的、有序的通信.

图2描述了Message queues的内部结构.在这个系统中,每个网络节点都运行一个 Agent server.当一个事件发生时,Channel 将事件封装到一个消息中,这个消息包含附加的逻辑时钟信息、发送者(sender)和接收者(listener)的唯一标识.然后,Channel 确定事件的目的地.如果事件的目的地不在本地,则将消息传给远程的

Channel. 远程的 Channel 将接收到的消息存入消息队列中,由消息队列来保证其先后序列. 一旦有接收事件,远程的 Channel 随即启动一个进程,将消息传给 Engine. 接着,这个消息由 Engine 恢复,以激活某 Agent 对事件作出反应动作. 当发生错误时,消息被自动存储在消息队列中. 这样,由 Channel 使用的内部排队很容易实现消息的恢复. 同时,消息的先后顺序也可由其所带的时钟信息来完成. 因此,消息和有序性即使在方式网络错误的时候也可以保证.

4 结 论

在本文中,我们引入了"Agent"的概念. 对防火墙系统中各部件进行"Agent"化的设计,规范了各 Agent 之间的通信. 通过这样的设计和实现,提高了防火墙系统的开放性和结构可伸缩性,为适应各种安全策略的要求提供了基础. 对用户提供了自动或半自动的用户化安全审计和重配置方式,这不但为防火墙系统本身提供了方便,而且也为基于防火墙的安全系统中的安全策略配置和安全管理的一致性提供了基础.

参考文献

1 Maes P. Modeling adaptive autonomous agents. Artificial Life Journal, 1994,1(1,2):135~162

2 Crosbie M, Spaord E. Defending a computer system using autonomous agents. In: Proceedings of the 18th National Information Systems Security Conference. 1995. 549~558

3 Crosbie M, Spaord G. Active defense of a computer system using autonomous agents. Technical Report 95-008, COAST Group, Department of Computer Sciences, Purdue University, 1995. http://www.cs.purdue.edu/homes/spaf/tech-reps/9508.ps

4 Balasubramaniyan J S, Garcia-Fernandez J O, Isacoff D *et al*. An architecture for intrusion detection using autonomous agents. Technical Report 98/05, COAST Laboratory Purdue University West Lafayette, IN 47907-1398, June 11, 1998. ftp://coast.cs.purdue.edu/pub/COAST/papers/diego-zamboni/zamboni9805.pdf

5 Check Point FireWall-1(tm) White Paper Version 3.0. Check Point Software Technologies Ltd., July, 1997. http://www.checkpoint.com

6 Zhang Hao han, Pan Zhi-geng, Shi Jiao-ying. A multi-agent based collaborative design system. Journal of Software, 1998, 9(supplement):98~102
(章昊翰,潘志庚,石教英. 基于多 agent 模型的协同设计系统. 软件学报,1998,9(增刊):98~102)

Design and Implementation of an Agent-Based Firewall System

ZHANG Lei QING Si-han

(*Institute of Software The Chinese Academy of Sciences Beijing* 100080)
(*Engineering Research Center of Information Security Technology The Chinese Academy of Sciences Beijing* 100080)

Abstract In this paper, the authors first analyze the common shortcoming in the existing firewall systems. Based on these, they introduce a new concept-Agent. According to the definition of Agent, they define some Agent-based components of a firewall, and then describe the communication and collaboration of the Agents. Finally, the course of designing and deploying an Agent-based firewall is presented.

Key words Firewall, Agent, IP filter, application proxy, security audit.