面向大型网络的防火墙系统设计

雷英杰[1]，赵　晔[1]，邓　宁[2]
(1. 空军工程大学 导弹学院，陕西 三原 713800;2. 空军雷达学院，湖北 武汉 430010)

摘　要:根据防火墙的固有弱点,提出了相应的解决方案。并根据大型网络的安全需要,综合包过滤Agent、入侵监测等技术设计了一种结合网络分析器和入侵检测的防火墙体系结构。该体系对于内外网络分别予以考虑,具备了内外兼防的能力,可有效防止安全攻击。

关键词:防火墙;入侵检测;Agent;网络分析器;包过滤
中图分类号:TP393　　**文献标识码**:A　　**文章编号**:1009-3516(2001)06-0034-03

防火墙一般采取固定的安全策略来分隔内外网络和对内部的充分信任,所以其本身存在较大的缺陷[1-2],主要表现为:1)对内部用户不加防范,而调查研究表明70%的网络攻击来自内部;2)由于入侵者不断搜寻新的入侵手段,而软件的Bug又不可避免,相对于固定的安全策略来说,防火墙对系统未发现的Bug所产生的问题无能为力。基于这两种情况,要求一个健壮的防火墙系统不但能使用静态的策略而且需要能对网络动态监控、动态配置。又因为内部网络各节点对安全的要求不同,在其结构上还要有一定的伸缩性和灵活性。鉴于上述原因,可设计一个结合通信分析器和面向Agent的入侵检测模型的防火墙系统[3]。

1　新型防火墙的基本设计思想

新型防火墙是面向大型网络防护的,设计思想体现于入侵检测、包过滤Agent模型和通信分析器[4]。

1.1　入侵检测

利用每个数据包所含有的特定信息包头,如IP地址、协议等,根据访问控制表决定其是否允许通过,称为包过滤。依靠捕获所有的网络传输,由系统对典型攻击分组比较及对重要数据和重要服务进行监控,按照一定的识别机制,判断是否遭到攻击,称为入侵检测。

本方案采取基于模式的入侵检测方式[5]。这种检测主要考虑事件序列的相互关系,例如:一台主机向服务器发SYN请求,紧接着应发ACK信号,如果一段时间内没有发ACK信号,则确认为攻击。

规则IF(E1! E2! E3!)THEN(E4=95% E5=95%),其优点是:1)能较好地处理变化多样的用户行为,具有很强的时序模式;2)集中考察少数几个相关的安全事件,而不是关注可疑的整个登录会话过程,较易实现;3)对发现系统遭受攻击,具有良好的灵敏度。

1.2　包过滤Agent模型

Agent是一个活动的、自治的、内部驱动的实体,能以主动服务方式完成一组操作,具有智能性、自主性、交互性和可移动性,能作用于自身和环境,并对环境作出反应。以事件触动机制完成任务。

1)包记录:对网络层每个包进行采集记录。

2)匹配:对活动记录按照一定的规则进行匹配,成功启动。

3)否则启动事件产生器,修改规则库。由于对规则知识库的不断更新,故可对不断变化的入侵手段进行有效防范。

4)事件记录:记录可疑事件,保存捕获的原始分组。提供报警信息,采取有效手段阻塞入侵主机。

收稿日期:2001-06-20
基金项目:军队重点科研项目基金资助
作者简介:雷英杰(1956-),男,陕西渭南人,教授,博士生导师,主要从事人工智能与专家系统、网络与信息安全技术研究.

包过滤 Agent 模型如图 1 所示。

1.3 通信分析器

通过对网络流量进行分析,查询数据包路由路径标志和 ICMP 的信息,为及时发现起始攻击源提供线索。

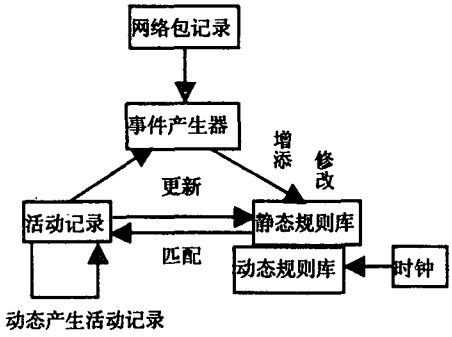

图 1　包过滤 Agent 模型

2 新型防火墙结构设计

新型防火墙结构如图 2 所示。该防火墙由内部网、外部网、中间停火区(DMZ)三个部分构成,由两个路由器分开。在不同的区域采取不同的安全措施。

在防火墙后的 DMZ 区,由于通信量大和面对外部网,故使用两个专门的服务器设立检测中心和网络分析中心;对于内部网,为灵活配置,使用具有包过滤自主功能的 Agent 在集线器前进行监测,由检测中心和各 Agent 构成网络入侵检测系统。

由于检测中心和各 Agent 之间的通信十分重要并防止入侵检测系统被攻击,需在它们之间建立隐蔽通道使其同公共网络分开[6]。同时,为防止其通信被修改,需要在检测中心设立验证授权中心,使用加 DES 数据验证消息的数据包进行通信。

当攻击者从外部攻击时,如果攻破了外部路由器和防火墙外层领域,只能得到一些无关紧要的访问机会,并未发现内部网络。如稍有不慎,将被入侵检测系统发现,阻塞其连接,同时网络分析器追查其位置。当面对分布式拒绝服务攻击时,在阻塞服务的同时,由网络分析器追查攻击者原位置。当攻击者从内部发动时,Agent 首先检查数据包的 IP 地址是否为本子网片段地址,如不是,首先阻塞其出口,防止本地用户使用源地址欺骗攻击其外的网络。同时,根据自身规则库判断是否出现攻击,如发现攻击,阻塞其出口,通知检测中心。由于 Agent 的规则库可灵活配置,故能适合不同网络片段的安全要求。同时,检测中心根据 IDS 的监测情况动态地配置内外路由过滤规则。

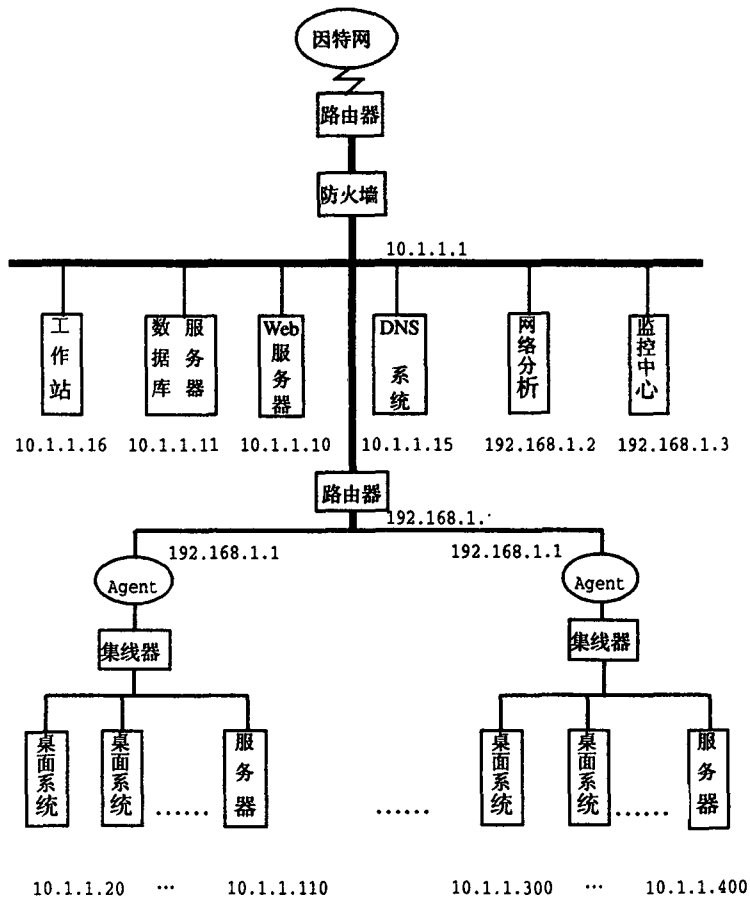

图 2　新型防火墙系统结构

3 新型防火墙中包过滤 Agent 实现

因包过滤 Agent 是一个自主实体,处理的通信量不大,所以可用专门的硬件和软件实现。软件可采取面向对象的设计方法设计。其对象应包括记录器、规则库、事件产生器、审记器、接收器、发送器、报警器、干涉器、验证生成器等。

限于篇幅,这里仅给出规则库对象的类结构:

```
Class rule
{
    private·
```

```
    int     IncidentID;          //事故标识号 ID
    int     ConditionNumber;     //条件数目
    char    *Condition[ ];       //指向条件的指针
    char    *Conclude[ ];        //指向结论的指针
    public:
    void    DelRule( );          //删除规则操作
    void    AddRule( );          //添加规则操作
    void    Next( );             //指向下一条规则链
    void    Check( );            //行使规则检查
}
```

4 隐蔽通道的建立

本方案的新型防火墙使用隐蔽通道主要是为了防止攻击者发现检测系统和修改其通信。其基本原理是:1)使用虚拟专用网络;2)使用加密通道;3)在 DNS 上使用两种 IP 地址分隔常规网和检测专用网络。

5 结论

新型面向大型网络的防火墙中引入面向 Agent 的入侵检测技术和网络通信分析技术,不但提高整个系统的灵活性和对攻击的免疫性[7],而且对内部用户起到警告威慑作用。在不同网络子网片段前使用 Agent,不但提高了对攻击反应的灵敏性,也保障各子网片段的相对分离,从而提高了系统的整体安全性能[8]。

参考文献:

[1] 蒋建春,马恒太,任党恩,等. 网络安全入侵检测:研究综述[J]. 软件学报,2000,11(11):1460 - 1466.

[2] Chris Brenton. 网络安全入门到精通[M]. 马树奇,金 燕. 北京:电子工业出版社,1999.

[3] 杨守君. 黑客技术与网络安全[M]. 北京:中国对外翻译出版公司,2000.

[4] 张 磊,卿斯汉. 一个基于 Agent 的防火墙系统的设计与实现[J]. 软件学报,2000,(5):642 - 645.

[5] 陈 硕,安常青,李学农. 分布式入侵检测系统及其认知能力[J]. 软件学报,2001,12(2):225 - 232.

[6] CERIAS,Purdue University,COAST EB/OL http://www. cs. purdue. edu/coast/projects/aafid. html.

[7] Deber H. Dacier M. Andreas wespi towards a taxonomy of intrusion - detection systems. Computer Networks[J]. 1999,31(8): 805 - 822.

[8] Sekar R,Guang Y,Verma,S. ,et al. A high - performance network intrusion detection system[A]. Tsudik,G ed. Proceedings of the 6th Conference on Computer and Communication Security[C]. New York:ACM press,1999. 8 - 17.

Design of a Firewall System Applied to Larger Networks

LEI Ying - jie[1], ZHAO Ye[1], DANEG Ning[2]

(1. The Missile Institute of the Air Force Engineering University,Sanyuan Shaanxi,713800,China;2. Air Force Radar Institute,Wuhan Hubei,430010,China)

Abstract:The limitation of a general firewall is analyzed,and some solutions of enhancing the security of networking systems are presented in this paper. According to the security necessity of larger networks,the paper synthesizes the techniques of packed - filtering Agent and intrusion detection sysytem,etc. ,and designs a new firewall system combined traffic sniffer and intrusion detection. The system considers inner and outer networks separately,and it has the capability of protecting both them from security attacks effectively.

Key words:firewall;intrusior detection;Agent;traffic sniffer;packet filtering