

基于入侵检测的分布式防火墙的应用研究

胡 平, 李 臻, 彭纪奎

(南京工业大学 电子与信息工程学院, 江苏 南京 210009)

摘 要: 针对分布式防火墙和入侵检测技术各自存在的不足, 文中提出基于入侵检测的分布式防火墙的解决方案, 通过在主机防火墙内部增加入侵检测模块, 形成一种动态分布式防火墙. 主机防火墙过滤模块通过修改数据包结构以减少入侵检测量, 入侵检测结果快速返回管理中心, 及时动态更新策略. 实验结果表明: 该方案解决了分布式防火墙策略更新慢、内部通信被非法用户截获、无法及时发现入侵攻击等问题, 同时也解决了入侵检测模块的数据检测量大和无法阻断攻击等问题.

关键词: 入侵检测; 网络安全; 网络数据拦截; 动态分布式防火墙

中图分类号: TP393.08

文献标识码: A

文章编号: 1000-7180(2011)06-0126-05

Application Research of Distributed Firewall Based on Intrusion Detection

HU Ping, LI Zhen, PENG Ji-kui

(College of Electronics and Information Engineering, Nanjing University of Technology, Nanjing 210009, China)

Abstract: In view of the deficiencies of distributed firewall and Intrusion detection, a distributed firewall based on Intrusion detection is proposed. It improves the architecture of distributed firewall by adding intrusion detection module in order to get a dynamic distributed firewall. It reduces the amount of intrusion detection data by modification the structure of packets when they arrive at the intrusion detection module from the host firewall filtering module. The results of data detection return to management center rapidly, so the management center can update rule dynamically and timely. The experimental results show that the proposed scheme solves some problems of traditional distributed firewall, including the policy updating delay, unauthorized users can intercept the internal communication and intrusion can not be found timely etc. Meanwhile, it also solves some problems of intrusion detection module such as the large amount of data, the inability of blocking the attack and so on.

Key words: intrusion detection; network security; networks data interception; dynamic distributed firewall

1 引言

随着计算机网络的广泛应用, 网络安全问题也变得越来越严重^[1]. 分布式防火墙技术和入侵检测系统已经成为解决网络安全问题的常用手段^[2]. 但是, 分布式防火墙因其受制于被动的、静态的防御特征, 在攻击识别和策略更新等方面仍然存在着很大缺陷^[3]. 入侵检测作为一种主动防御的安全技术, 在发现入侵和报警响应等方面取得了一定的成果, 但

是由于高速网络带来的大量数据使得数据检测效率低下和无法及时阻断攻击等也制约着入侵检测的进一步发展.

文中针对两者各自的缺点, 对分布式防火墙体系结构做了一定改进, 在主机防火墙内部增加入侵检测模块, 策略管理中心结合入侵检测及时发现攻击得到的信息能够及时自动更新分布式防火墙的过滤规则, 形成一种动态分布式防火墙 (Dynamic Distributed Firewall, DDFW).

2 DDFW 的总体结构

根据动态分布式防火墙的基本要求^[4-5],文中设计出的 DDFW 系统体系结构,如图 1 所示。

接收数据时,主机防火墙首先从网络中获取网络封包,经主机防火墙策略执行器过滤数据,再上传至入侵检测中心;入侵检测中心在检测过程中若发现攻击则反馈信息给管理中心,管理中心快速制定

策略,发送至各个主机防火墙。应用程序访问网络时,主机防火墙拦截应用程序进程,策略执行器根据进程信息来匹配网络访问规则,加密通信等网络安全防范措施作为 DDFW 内部通信的安全基础。在动态策略管理控制中心的指导下,各个模块相互协调,入侵检测系统内嵌进主机或边界防火墙内进行数据分析检测,对网络入侵行为和动态网络弱点漏洞、非法使用和不正确的操作进行响应。

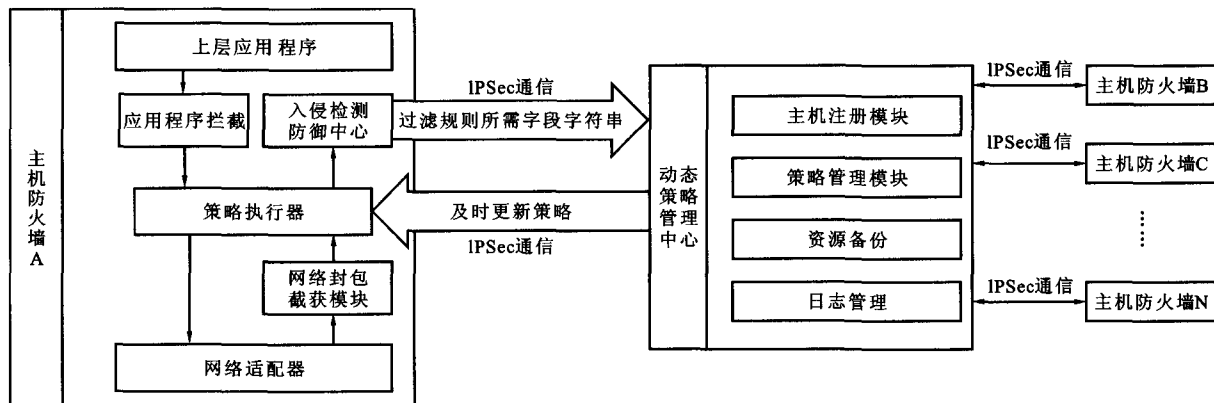


图 1 动态分布式防火墙体系结构

3 DDFW 关键技术分析

3.1 防火墙数据拦截技术

数据拦截技术对操作系统平台的依赖性很强,文中主要论述针对 Windows 操作系统平台的网络数据截获技术。

在 Windows NT 结构下进行网络数据包拦截技术可以分为用户模式和内核模式两种情况:

(1) 用户模式下拦截网络数据包的优点是可以获得调用 Winsock 的进程的详细信息,编程简单、安装容易。缺点是一般只能在 Winsock 层次上拦截数据包。

(2) 内核模式下进行数据包拦截可以在 TDI 层和 NDIS 层这两个层面上进行。

① TDI 过滤驱动数据拦截技术

TDI 过滤驱动的优点是能够取得被拦截进程的信息,缺点是一些木马、病毒等攻击程序可以直接绕过 TDI 层,因此 TDI 过滤驱动无法拦截所有数据。

② NDIS 中间驱动数据拦截技术

NDIS 模型允许在协议驱动程序与网络适配器驱动程序(小端口驱动程序)之间插入分层驱动程序,这种分层驱动程序称为 NDIS 中间层驱动程序。系统中所有的网络通信都经过 NDIS 中间层驱动程序,它工作于网络层和数据链路层之间,因此它可以

用于所有网络数据包的拦截与过滤。由于 NDIS 层次上的网络操作不采用标准的 I/O 模式,因此不能确定引起该网络操作的进程信息。

根据数据包拦截技术的一些优缺点,考虑到系统的效率、功能实现及可扩展性等,本系统采用 TDI 过滤驱动程序和 NDIS 中间驱动程序技术相结合的方式开发防火墙拦截模块。

3.2 分布式防火墙与入侵检测联动技术

目前防火墙与入侵检测存在两种联动方式^[1]:一是通过开放接口实现互动,即防火墙产品和入侵检测系统产品开放一个接口供对方调用,按照相互规定好的协议结合;二是防火墙技术和入侵检测与集成到同一个系统内,在统一管理和控制之下有序地运行。

文中将入侵检测系统嵌入到分布式防火墙的各个实施点(主机/网络边界防火墙)中,实现入侵检测模块和防火墙过滤模块的紧密联系。防火墙过滤模块成为第一道防线,入侵检测模块成为第二道防线,入侵检测模块数据来源不再是直接来源于网络层,而是已经流经防火墙过滤模块的数据流。所有接收到的网络封包在经过防火墙的检测规则的验证之后,被包装成特定数据结构的数据包传至入侵检测模块检测是否带有攻击数据,以达到实时的检测和阻断并存。

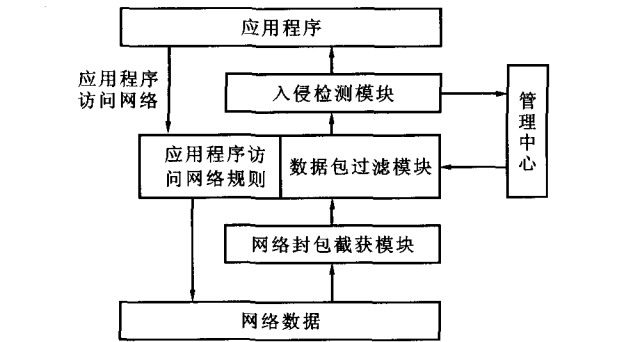


图 3 主机防火墙体系结构

NDIS 中间驱动程序技术相结合的方式实现,本模块包含两部分,一部分为 NDIS 中间驱动程序对网络接收数据包的拦截,另一部分为 TDI 过滤驱动程序对应用程序访问网络的拦截。

NDIS 中间驱动程序负责拦截并分析所有通过网络适配器到达系统的数据包,在拦截所有数据包之后根据过滤规则,完成对所有数据包的拆分匹配,以确定是否危险数据包,根据匹配规则选择不同行为,放行或丢弃。

TDI 过滤驱动程序拦截所有应用程序访问网络的进程,提取进程信息,经防火墙过滤模块进行程序访问控制,以确定该进程被用户是否设置为是否能够访问网络。

数据拦截模块的结构如图 4 所示。

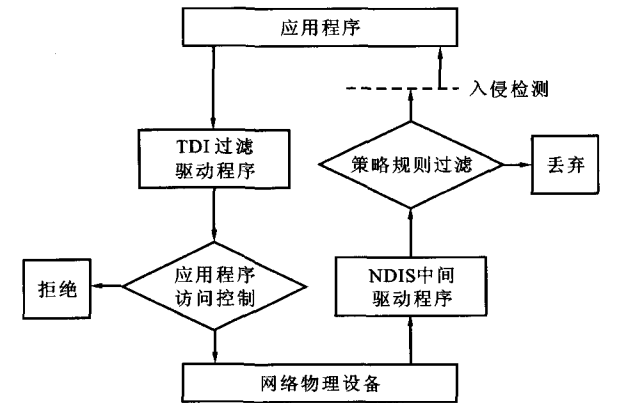


图 4 防火墙的数据拦截过程

5.2 策略执行器的设计

主机防火墙的策略执行器主要分为接收数据过滤和应用程序访问网络的进程控制过滤两大模块。接收数据过滤时,在接收并重组网络完整封包之后解析数据包,取得相关包头信息,根据策略规则文件来判断该数据包是否放行,如果规则是放行,则指示上层入侵检测模块接受数据,否则直接拒绝。应用程序访问网络进程过滤时,TDI 过滤驱动程序拦截应用程序并取得进程信息,根据已经初始化完成的应

用程序访问网络控制表的信息来决定是否放行该进程对网络的访问。如果控制表中没有该进程信息,则提示用户设置新的访问规则。策略执行器的流程如图 5 所示。

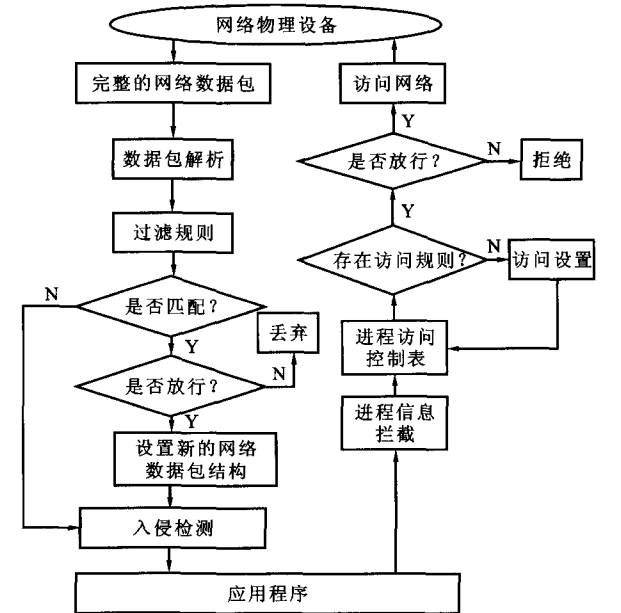


图 5 策略执行器模块流程图

5.3 入侵检测中心设计

入侵检测中心不但能检测入侵的发生,而且能通过一定的方式提示分布式防火墙的策略管理中心采取措施,及时地阻断入侵行为,保护系统的信息安全。入侵检测中心同一般入侵检测系统一样专注于前瞻性的防护,其设计宗旨是对防火墙过滤的有效补充,目的在于对入侵活动和攻击性网络流量进行预先拦截。模块结构如图 6 所示。

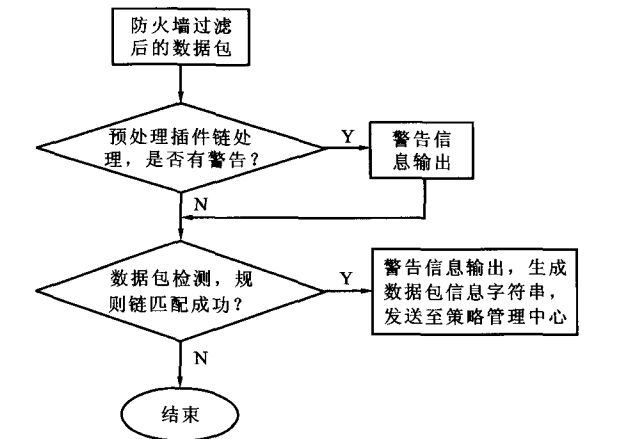


图 6 入侵检测模块流程图

6 实验分析

DDFW 测试使用了 5 台计算机,系统平台采用

Windows XP SP2, 入侵检测规则数据库为 MySQL5. 1. 3. 其中一台作为系统外部主机, 作为攻击源进行测试, 一台作为分布式防火墙管理控制中心服务器, 其余三台作为分布式防火墙的策略执行主机. 具体配置情况如表 1 所示.

观察监控中心对主机防火墙流量检测, 查看其通信记录, 测试系统的 IPSec 加密通信.

观察结果表明系统内部的主机之间、主机与策略管理中心之间的通信全部完成了 IPSec 通信加

密, 不用担心外部监听拦截等.

从攻击机运用端口扫描工具 X-Scan3. 0 向主机服务器管理中心进行扫描攻击, 观察监控中心警告信息以及防火墙动态策略更新和响应时间时间变化. 从测试结果可以看出, 防火墙从察觉被端口扫描到发现入侵木马到中断入侵攻击机连接, 整个过程时间在 9 秒内, 达到了动态防火墙及时自动更新策略的要求.

表 1 测试环境配置情况

IP 地址	作用分配	系统配置
202. 119. 242. 206	动态策略管理服务器	WindowsXP SP2+MySQL5. 1. 33
202. 119. 242. 207	策略实施主机 A	WindowsXP SP2+MySQL5. 1. 33
202. 119. 242. 227	策略实施主机 B	WindowsXP SP2+MySQL5. 1. 33
202. 119. 242. 154	策略实施主机 C	WindowsXP SP2+MySQL5. 1. 33
202. 119. 242. 197	测试攻击源	WindowsXP+测试工具 X-scan 等

对入侵特征文件所定义的一些入侵攻击, 如 UNICODE 漏洞攻击、IIS 溢出攻击、IMAP 溢出攻击、Back Orifice2000 木马、Win Terminal Server 木马、DoS(拒绝服务)攻击等进行数据实验测试系统性能, 攻击测试结果如表 2 所示.

表 2 攻击包分类及测试结果

攻击名称	攻击包数	阻断数	误报个数	漏报个数
UNICODE 漏洞攻击	210	213	8	15
IIS 溢出攻击	134	129	16	21
IMAP 溢出攻击	64	67	11	8
Back Orifice 木马	76	72	12	16
Win Terminal Server	42	64	27	5
DoS	148	143	28	23

根据统计结果可以看出, 入侵检测模块在防火墙过滤模块的联动机制下误报率为 16. 62%, 漏报率为 13. 05%. 共发送数据包总数 50 万个, 防火墙接收到数据包 497347 个, 丢包率 5. 36%. 主机防火墙因为入侵规则改变而系统阻断入侵包个数 668, 误报包个数为 112, 系统成功阻断包总数 556, 因此系统实际丢包率为: $1 - 497347 / (500000 - 556) = 4. 20\%$.

7 结束语

文中根据分布式防火墙和入侵检测的特点, 改

进现有的分布式防火墙模型, 设计并实现了一个融合入侵检测模块的动态分布式防火墙系统框架. 实验结果表明, 该方案不但具备分布式防火墙在阻断攻击方面的优点, 同时具备了入侵检测系统在实时发现攻击方面的功能.

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—1467.
- [2] 戴硕, 杜晔. 一种异构分布式防火墙与入侵检测联动构架的通信机制[J]. 微电子学与计算机, 2009, 26(8): 94—97.
- [3] 赵戈, 钱德沛, 范晖. 用分布式防火墙构造网络安全体系[J]. 计算机应用研究, 2004, (2): 106—107.
- [4] Ioannidis S. Implementing a distributed firewall[C]// Proceedings of the ACM Conference on Computer and Communications Security, NY, USA: ACM, 2000: 190—199.
- [5] 戴宝鑫. 一个分布式防火墙防火墙系统的设计于实现[D]. 沈阳: 东北大学, 2006.

作者简介:

- 胡 平 男, (1962—), 副教授. 研究方向为网络安全.
- 李 臻 男, (1984—), 硕士. 研究方向为网络安全.
- 彭纪奎 男, (1982—), 硕士. 研究方向为网络安全.