IPv6 防火墙过滤技术的研究与应用

袁伟云[1],聂瑞华[1,2],梁卓明[2],梁 军[2],李 艳[1]
(1.华南师范大学 计算机学院,广东 广州 510631;
2.华南师范大学 网络中心,广东 广州 510631)

摘 要:由于IPv6协议格式自身的特点,使得传统的IPv4防火墙不能很好地应用于IPv6网络,故对IPv6防火墙技术的研究成为了一个热点。为了使传统的IPv4防火墙能够更好地适应用于IPv6网络,从防火墙的过滤技术入手,分析比较几种主要的过滤技术及其特征,将流过滤技术引入IPv6的防火墙中,结合了Linux下开源防火墙NetFilter框架,给出了流过滤技术在IPv6防火墙中具体的实现思路与方法,最后对这种流过滤防火墙的性能进行测试,表明了IPv6流过滤防火墙的可行性。

关键词:防火墙;过滤;TCP/IP协议栈;规则链表
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2010)09-0145-04

Research and Application of Filtering Technology on IPv6 Firewall

YUAN Wei-yun[1], NIE Rui-hua[1,2], LIANG Zhuo-ming[2], LIANG Jun[2], LI Yan[1]
(1. School of Computer, South China Normal University, Guangzhou 510631, China;
2. Network Center, South China Normal University, Guangzhou 510631, China)

Abstract: Because of IPv6 protocol its own characteristics, make the traditional IPv4 firewalls are not well adapted to IPv6 network. Research on IPv6 firewall technology has become a hot spot. In order to make the traditional IPv4 firewalls are better able to adapt to the IPv6 network, starting with analysising and comparing several filtering technologies and their characteristics, then flow filtration technology is introduced into IPv6 firewall, on the basis of the open-source firewall framework-NetFilter in Linux, the specific idea and method of flow filtration technology in the IPv6 firewall is given, finally the performance of this flow filtration firewall is tested, demonstrats the feasibility of IPv6 flow filtration firewall.

Key words: firewall; filtration; TCP/IP protocol stack; rules chain

0 引 言

IPv4网络向IPv6网络过渡,IPv4的防火墙不能很好地适应IPv6网络,主要是由以下两个方面的原因[1]:

(1) IPv6的结构,IPv4的IP报头和TCP/UDP报头紧接在一起,且长度基本固定,防火墙过滤模块很容易找到IP地址和TCP/UDP端口信息从而进行过滤;而IPv6的扩展报头存在于IP基本报头与TCP/UDP报头之间,对过滤模块与过滤函数寻找IP地址及TCP/UDP中的端口信息带来麻烦,这样导致IPv4过滤与IPv6过滤方式存在差异。

(2) IPSec是IPv6必须的功能,如何过滤经过加密的数据是IPv6防火墙必须解决的又一问题。过滤技术是防火墙的核心,研究适合于IPv6防火墙的过滤技术,成为了一个热点。

1 现有的几种过滤技术及其特征

1.1 静态包过滤技术

静态包过滤技术[2]是通过一定的过滤规则来决定数据包的过滤和转发,过滤规则是基于数据包的报头中的IP地址、TCP/UDP源端口、TCP/UDP目的端口等,包过滤的优点是实现简单,缺点是综合安全性低。

1.2 状态检测包过滤技术

状态检测包过滤技术[2]是一种动态的包过滤技

收稿日期:2009-12-29;**修回日期**:2010-03-26
基金项目:国家教育科研基础设施IPv6技术升级和应用示范项目(CNGI2008-084)
作者简介:袁伟云(1984-),男,湖南衡阳人,硕士研究生,研究方向为计算机网络与应用技术;聂瑞华,教授,研究方向为计算机网络及应用、网格计算。

术,是对静态包过滤技术的一种改进,是一种基于状态的包过滤检测机制,它通过在内存记录一个状态表,状态表是动态变化的,从而使已建连接的数据包通过匹配状态表决定过滤与否。状态检测包过滤优点是性能与安全性高。

1.3 应用代理过滤技术

应用代理过滤技术[2]是阻止访问者与服务端建立直接的 TCP 连接,隔断直接通信。所有通信都通过应用层的代理转发,应用代理的优点是应用层的控制能力强,缺点是难于配置,处理速度慢。

2 流过滤技术介绍

2.1 流过滤技术的概念与原理

流过滤[3]的概念是由东软提出来的,其基本原理是在状态检测包过滤的基础上,采用专门的 TCP/IP 协议栈,在应用层实现对链路层的数据流重组,将重组过后的数据流交给防火墙的过滤模块,从而完成过滤。

2.2 流过滤技术的实现原则与步骤

1) 数据包捕获。

基于 Linux 下面的 TCP/IP 协议栈进行数据包的获取,Linux 协议栈的一个核心数据结构 sk-buff,对所捕获的数据包进行分析,并按照 IP 地址与包结构,提取 IP 数据包的特征信息,数据包的捕获是过滤的前提与基础。

2) 发送报文应答[2,4]。

为了保证发送方与接收方的数据传输能够顺利进行,防火墙在接收到发送端的报文后给发送端发送报文确认,这个报文确认是由防火墙直接发往发送端(代替接收端发送),所使用的连接是伪装连接(用接收端的端口与 IP)。具体体系结构如图 1 所示[4]。

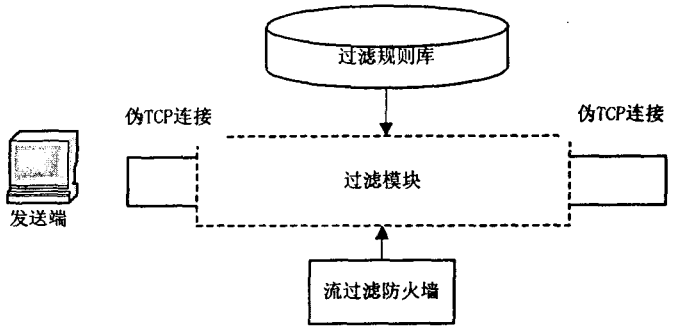

图 1 流过滤体系结构

3) 获取会话报文链。

对报文中的相关键字(报文的源 IP、源端口、目的 IP、目的端口)做 Hash 函数处理,通过所得的 Hash 函数值来判断报文是否属于同一会话,属于同一会话报文构成一条会话报文链。

4)报文链处理。

报文链处理是对会话报文链进行人工处理,以解决报文链中的乱序与重复的问题,具体的解决方法是按报文结点中的序列号进行排序,然后按序列号过滤掉重复报文,从而构成了有序非重复报文。处理过程如图 2 所示[2,4]。

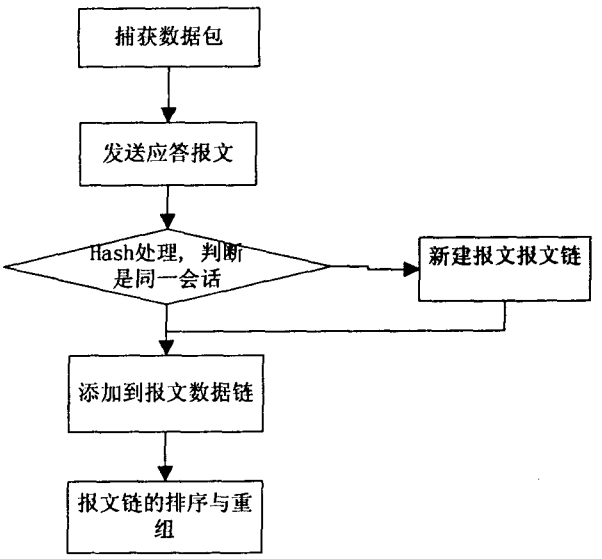

图 2 报文数据的处理流程

5) 数据的过滤与转发。

对处理后的报文数据进行流过滤规则匹配与转发,流过滤规则中除含有一般的过滤规则(基于源 IP 地址、目的 IP 地址、源端口、目的端口的过滤)外,还应针对特定应用增加额外的过滤规则(比如基于关键字的内容过滤),以便更好对不同的应用实现流过滤,最后,防火墙将完成过滤的合法报文按原始的顺序(即报文链)发送给接收端,从而完成过滤与转发。具体的流程如图 3 所示。

3 流过滤技术在 IPv6 防火墙中的实现

为解决 IPv6 报文加密数据的过滤,IPv6 防火墙采用一种屏蔽子网的防火墙系统结构[5],其关键模块是过滤模块(基中包括了包过滤与流过滤),流过滤模块中主要涉及以下几个方面:会话报文数据的重组与排序、数据的过滤、合法数据的转发。

3.1 IPv6 流过滤相关的数据结构的设计

(1) 会话报文数据的重组与排序。

会话报文数据的重组就是将同一会话中的关键报文组合在一起,同一会话报文的数据按发送的顺序存储在同一个链表中,会话报文链表[6]数据结构具体定

义如下:

```
Struct sessionPacketNode
{
```

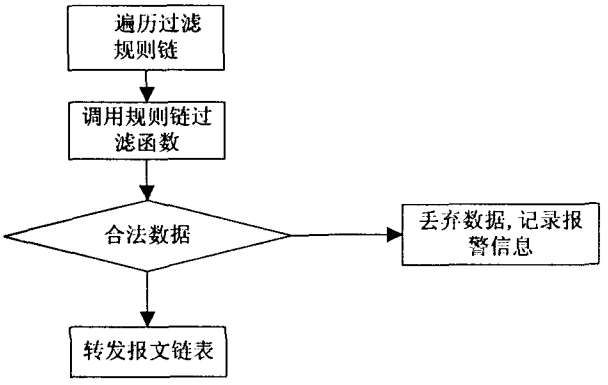

图 3　流过滤流程

```
Int sequence; //报文序列号
struct ip6t_ip6 * ipv6h //IPv6 报头数据结构,内含 ipv6 报文的源、目的地址信息
struct ip6t_tcp * ipv6tcp //IPv6 TCP 头数据结构,内含 ipv6 报文的源、目的端口信息
struct ip6t_udp * ipv6udp //IPv6 UDP 头数据结构,内含 ipv6 报文的源、目的端口信息
struct ip6t_icmp * ipv6icmp //IPv6 ICMP 头数据结构
char * packetData; //报文数据指针
sessionPacketNode * next; //下一个报文结点的指针
}
```

对于一个会话,新建一个链表,对于一个新到报文,若与当前会话报文链属于同一会话,将报文加入到当前会话报文链表中;若不属于当前会话报文链,则新建一个报文会话链表,这样同一会话报文数据就可以用一个链表存储与表示。同时,将链表中重复结点从链表中删除,过滤了重复报文;按序列号字段对链表进行排序,从而构成了一个有序的报文链。

(2)流过滤。

流过滤就是对重组后的会话报文进行匹配过滤的一个过程,在流过滤中要设计两个数据结构,一个是功能链表,主要处理防火墙中一类功能操作,每一个结点表示不同的功能类型,多个功能结点构成功能链表,具体的定义如下:

```
Struct EffectNode
{
Int EffectID; //功能 ID
String EffectName ; //功能类型名称
ruleNode * rule; //指向规则链表的首指针
EffectNode * next //指向下一个功能结点
}
```

另外一个是规则链表,主要存储一种类型功能操作中的若干条规则,用户根据需要,可以自定义或编辑规则链表,在数据过滤功能中,数据报文可以遍历该过滤功能结点所对应的规则链表,从而完成特定报文的过滤,规则链表[7]具体的定义如下:

```
Struct ruleNode
{
Int ruleID; //规则 ID
String ruleName; //规则名称
Int * Filter(sessionPacketNode * s1, patternNode * s2); //规则所对应功能函数的指针(以 Filter 表中规则为例,其所对应的功能函数为过滤函数)
Char * keyword1; //关键字 1(可以是过滤关键字,地址转换中源、目的地址等)
Char * keyword2; //关键字 2(可以是过滤关键字,地址转换中源、目的地址等)
ruleNode * next; //指向下一结点的指针
}
```

一条过滤规链则对应一个过滤函数,功能链表与规则链表的关系[8]如图 4 所示。

流过滤的过程是对报文数据遍历过滤功能结点所对应的规则链,去匹配不同的过滤规则,调用不同的过滤函数,同时根据过滤函数的返回值作相应处理(转发数据或丢弃数据),从而完成数据报文的过滤。

(3) 合法报文转发。

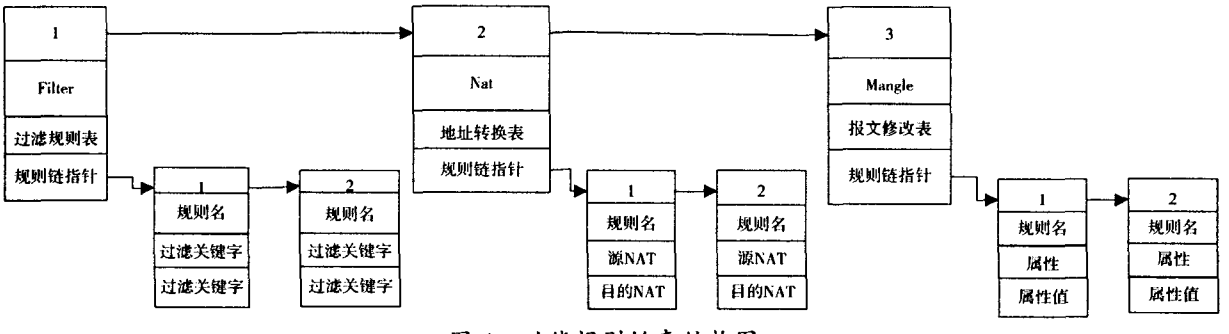

图 4　功能规则链表结构图

若报文链中的数据在遍历相关的规则链表(过滤函数),若没有发现相关的异常,则称为合法数据,合法数据的转发依然要依赖于 TCP 连接,继续启用报文重组过程中的维持连接(伪连接),就可以完成报文数据链合法报文的转发。

3.2 流过滤函数的实现

一条过滤规则对应一个或若干个过滤函数,其主要的功能是基于会话报文数据流实现过滤,文中基于基本的字符过滤算法[9],结合上面所给的数据结构,给出一个流过滤函数实现伪代码。

```
Int Filter(sessionPacketNode * shead, patternNode * phead)
//将报文链与规则链中过滤关键字作为输入参数
PatternNode q=shead;
sessionPacketNode p=phead;
while(p.next&&q.next) // 报文链与关键字链非空
{
if(p. packetData==q.patternData) // 若匹配成功,指针后移
{ p=p.next; q=q.next; }
else // 若匹配失败,则关键字链回朔到头结点
{ p=p.next; q=phead; }
if(q==null) return 0; // 报文链中含有关键字链内容,则说明存在非法数据,此时要返回 0,丢弃报文,保存报警信息
else return 1; // 合法数据,进行数据报文链中数据的转发
}
}
```

其中 patternNode 是过滤函数中的一个链表,结构与 sessionPacketNode 基本类似,用来存储过滤的关键字(IP 地址、端口、过滤内容等信息),不同的过滤函数 patternNode 链表内容不同,在过滤的实现过程中,只要对同一会话的报文链进行遍历就可以了,时间复杂度为 o(n)。

3.3 实验与性能分析

文中的实验环境是基于 Linux kernel 2.6 的防火墙开源框架 NetFilter,基于 NetFilter 实现非关键报文的包过滤,同时重写流过滤函数,将相关的过滤函数添加到规则链表中,同时将所重写的过滤函数注册到 NetFilter 钩子函数上,报文链数据流经 NetFilter 钩子时,遍历规则链,调用过滤函数,实现防火墙的流过滤[10]。在防火墙性能测试方面考虑采用 Iperf,Iperf 是一个网络性能测试工具[11],可以测试 TCP/UDP 带宽质量。Iperf1.7.0 支持 IPv6 流量产生,测试流过滤防火墙在 IPv6 环境下随着过滤规则增加带宽,丢包率,抖动的情况,具体的 IPv6 流过滤防火墙与 Iperf 部署的拓扑图[12]如图 5 所示。

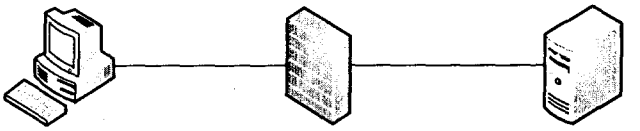

图 5 防火墙性能测试拓扑图

基于这种数据结构实现的过滤技术,所有的 IPv6 报文数据不再是以单独的方式进行匹配,而是以一种基于会话"数据流"[13]的形式进行安全检查,因此,安全性更高,同时,针对不同应用层协议构造一个协议链,可适用于应用层不同的报文数据,重用性与灵活性更高。

4 结束语

流过滤技术综合了包过滤技术与代理防火墙技术的优点,流过滤技术中实现了包数据重组成流数据块,而流数据块的过滤可以为应用层提供保护,解决了普通包过滤安全性差、不能控制应用层安全的缺点[4]。同时,流过滤防火墙对于具体的应用层协议只需要定义专门的规则链,重写对应的过滤函数即可,实现与部署灵活,相对简单。解决了应用代理防火墙中具体的应用层协议实现,部署困难的缺点。

文中分析比较了几种防火墙过滤技术特征,研究了流过滤防火墙实现原理与技术基础,将流过滤技术引入到 IPv6 的防火墙中,并给出了具体的设计方案与实现思路。模式匹配过滤算法的改进与优化,IPSec 与 IPv6 防火墙的结合将是下一个研究方向。

参考文献:

[1] 陈 雷,张志刚,肖文曙,等 .IPv6 防火墙的设计与实现[J].微计算机信息,2005,21(3):63-65.

[2] 胡志军.基于流过滤技术的 Linux 防火墙研究[D].成都:成都理工大学,2005:26-30.

[3] NetEye 3.1 防火墙技术白皮书[M].沈阳:东软软件股份有限公司,2003.

[4] 耿凤瑞,高仲合,李红伟.防火墙流过滤技术的分析与研究[J].计算机安全,2009,2(1):57-59.

[5] 王常杰,秦 浩,王育民.基于 IPv6 的防火墙设计[J].计算机学报,2001,24(2):219-223.

[6] Linux IPv6 Firewall project[EB/OL].2009-12-20.

(下转第 152 页)

改进可以减轻管理员的工作量。

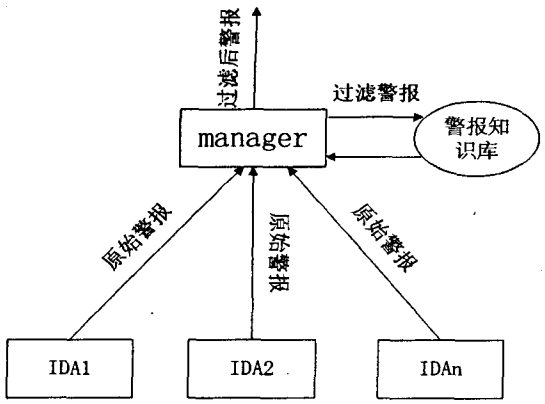

图 3 警报过滤模块

模型的第三层是 MANAGER,它的主要作用是向用户提供检测结果并管理、维护整个系统。检测结果中还包括受系统保护的特殊信息,这些系统数据在发现被攻击造成损坏的区域时非常有用,收集的数据类型包括使用的网络带宽、CPU 使用情况、网络数据包、内存使用情况、连接的数目、试图连接数目、协议、源端口与目的端口的比率和数据包的长度等。这些数据还有利于对系统内部的信息进行检测处理,可以根据这些信息的使用情况与平时的使用情况进行比对,如果发现异常就极有可能是内部发生入侵行为。

5 结束语

入侵检测作为一种积极主动的安全防护技术,提供了对系统的实时保护,能够在系统受到入侵时成功地响应报警,受到用户的好评。发展到今天各种各样的入侵检测系统凭借自身的优点在市场上不断发展,文中在探讨了几种常见的系统的优缺点之后,在保留分布式层次结构的基础上采用移动代理技术来克服收集节点地址固定的缺点,并对代理缺乏通信管理、不能共享数据、误报率高的缺点进行了研究改进,取得了一定的成果。

面对日益发展的网络和网络攻击手段的多样化,单凭现在的检测系统是无法满足用户的需求的。随着智能技术的发展,比如神经网络、智能算法的发展,入侵检测系统也有必要借鉴这方面的技术[12],来扩大自己的检测能力。相信未来的入侵检测系统必将克服现在系统的缺点,更好地保护系统的安全。

参考文献:

[1] 陈雪斌,刘 峰,赵志宏,等.安全的分布式入侵检测系统框架[J].计算机工程与设计,2009,30(14):3266-3268.

[2] 徐国芹.基于 AGLET 的分布式入侵检测系统的研究[J].赤峰学院学报:自然科学版,2009,25(5):28-30.

[3] 李 生,邓一贵,唐学文,等.基于移动代理的分布式入侵检测系统的研究[J].计算机技术与发展,2009,19(9):132-135.

[4] 项 目,杨小平.基于移动代理的分布式入侵检测系统模型[J].计算机工程与应用,2006(19):140-143.

[5] 肖 昆,郑 记.一种新型的适应于 MANET 的基于移动代理的对等入侵检测系统[J].计算机应用与软件,2007,24(4):157-159.

[6] 张淑英,刘淑芬.基于移动代理的多层次分布式入侵检测网络预警系统[J].计算机应用研究,2006(5):13-15.

[7] 李旭晖,吕 慧,向剑文.移动代理系统的安全问题[J].计算机应用,2001,21(7):5-8.

[8] 安 娜,张 凡,吴晓南.一个基于移动 Agent 的分布式入侵检测系统[J].西北大学学报,2005,35(1):25-28.

[9] Athanasiades N, Abler R, Levine J, et al. Intrusion detection testing and benchmarking methodologies[C]//Proceedings of the IEEE Information Assurance Workshop. [s. l.]:[s. n.], 2003:63-72.

[10] Antonatos S, Kostas G, Anagnostakis, et al. Generating realistic workloads for network intrusion detection systems[C]// Proceedings of the fourth international workshop on Software and performance. [s. l.]:[s. n.], 2004:207-215.

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

[12] 张雪芹,顾春华,林家骏.入侵检测技术的挑战与发展[J].计算机工程与设计,2004,25(7):1096-1099.

(上接第 148 页)

http://lxr.oss.org.cn/source/net/ipv6/.

[7] 孙冰心,张凤斌,江子扬. Linux 下内容过滤的实现[J].哈尔滨理工大学学报,2004,9(2):56-59.

[8] NetFilter project[EB/OL]. 2009-12-20. http://www.netFilter.org/.

[9] 严蔚敏,吴伟民.数据结构[M].北京:清华大学出版社,2002.

[10] 王一平,韦 卫.网络安全框架 NetFilter 在 Linux 中的实现[J].计算机工程与设计,2006,27(3):439-468.

[11] Iperf project[EB/OL]. 2009-12-20. http://sourceforge.net/projects/iperf/.

[12] 高鸿峰,王一波,傅光轩. NetFilter 框架下 IPv6 防火墙的设计与实现[J].电子科技大学学报,2007,36(6):1427-1429.

[13] 申凤兰.防火墙中透明模式和流过滤技术的研究与实现[D].广州:暨南大学,2003:22-23.