一种状态检测防火墙的攻击防御机制

阎 波，李广军

(电子科技大学通信与信息工程学院 成都 610054)

【摘要】讨论了一种在Linux操作系统内核防火墙的攻击防御机制，提出了检测网络攻击的机制和总体架构。在Linux操作系统防火墙的基础上构建了攻击防御框架，针对不同的攻击模式，该框架提供相应的状态检测方法判定攻击的发生并使攻击不能成功。提出的攻击防御体系具有通用、可扩展的特点，可以有效克服传统包过滤防火墙在抗攻击和入侵检测方面的局限性。结果表明：该攻击防御机制可以显著改善防火墙系统的IP安全性。

关 键 词 Linux操作系统； 状态检测； 防火墙； 网络攻击； IP安全性

中图分类号 TP309 文献标识码 A

An Attack Defense System Based on State Detection Firewall of Linux

YAN Bo，LI Guang-jun

(School of Communication and Information Engineering, UEST of China Chengdu 610054)

Abstract The principle of attack defense realized in a firewall embedded in Linux kernel has been discussed. Based on the analysis of characteristic of network attack, the mechanism and architecture of attack defense are built in accordance. Through the introduce of stateful detection, the attack defense framework is built to determine and prevent the deportment of various attack. Thereafter, the architecture of attack-removed system can be expected to be general-purpose and easy to be extended. The performance of the whole firewall system is enhanced because the attack defense system effectively overcomes the limitation of conventional packet-filtering firewall. The experiments for validating the improvement of IP security are given as well as the research work.

Key words Linux operate system; stateful detection; firewall; attack; IP security

根据网络攻击的常见步骤，网络攻击划分为：收集信息攻击、拒绝服务攻击DoS、获取访问权限攻击三种类型[1]。在各种防火墙技术中，包过滤防火墙的速度是最快的[2]。它的主要问题是：数据包的信息有可能是伪造的，此时如果满足过滤规则，防火墙也要放行。另外由于没有足够的上下文信息，包过滤防火墙也不能抵御SYNFlood攻击等基于连接的攻击[3]。本文引入状态检测技术提出了一种新的攻击防御机制，可以改进包过滤防火墙的攻击防御能力。状态检测的基本思想是在网络层拦截输入包直到有足够的企图连接的状态信息以作出判断。状态检测模块把从包中检测的状态信息保存在为评价后续连接企图的动态状态表中。由于检测发生在Linux操作系统内核，所以速度仍然很快。

收稿日期：2005－03－14

作者简介：阎 波(1973－)，女，硕士，讲师，主要从事可编程ASIC和计算机通信等方面的研究.

1 攻击防御的实现

本文讨论的攻击防御是指，根据用户的配置激活防火墙中相应的防御机制，从而使相应的网络攻击不能成功，以达到保护受信子网的目的。防御的目的是通过事先的准备使攻击不能成功，而不是阻止攻击的发生。根据对攻击原理的分析和抽象，本文实现的攻击检测和防御技术包括：

1) 协议分析机制。根据防火墙配置要求，对协议的首部信息进行分析，满足某种特征的，可以怀疑是攻击。

2) 时间分析机制。很多攻击表现出强烈的时间间隔特征，例如端口扫描，地址扫描，各种Flood攻击。对于这类攻击，应当对数据流中的两个包之间的时间间隔进行分析，判断是否满足时间阀值的要求。如果满足，则可以怀疑是攻击数据流。

3) 连接代理技术。主要针对面向连接的协议。例如，TCP连接请求超出临界值时，由防火墙代理连接请求，将攻击行为遏制在网络边界。

4) QoS流量工程。通过对(IP五元组，IP分片标志，TCP标志)定义的IP流应用QoS流量限速策略，可以丢弃过量的特定类型报文，保护受信子网不被淹没。

在攻击防御架构上合理组合、扩展这些攻击防御机制，是防火墙攻击防御体系能够保证安全和强有力的关键。

2 基于状态检测的网络攻击防御框架

2.1 状态检测防火墙的主要模块

本文实现的防火墙体系是在基于Linux定制的安全操作系统基础上，由基于状态检测的访问控制子系统，NAT子系统、攻击防御子系统等构成。这些防火墙子系统通过NetFilter机制[4]，挂接在IP协议层工作，如图1所示。其基本的处理过程是：

1) IP层首先把到来的包交给状态检测模块处理。状态检测模块判断包状态并存储在包的报文结构中；

2) 经过状态检测处理后的包由访问控制模块进行过滤。访问控制模块依据事先配置的规则与包的状态进行判断，决定是否丢弃包或者应用某种防火墙策略；

3) 通过过滤的包交由NAT模块进行处理；

4) 处理完毕的包最后又交给IP层处理、转发。

以上过程中，状态检测是实现防火墙的关键过程。它在内部维护一个连接表，负责根据到来的包驱动每一个连接的状态变换，并将该包与相应连接的关系存储在包的报文结构中。本文采用连接跟踪技术实现状态检测，它基于每一条连接记录对应的连接状态，并提供给各模块查询，以防止某些针对协议的攻击，拦截某些不合法的报文等。它也保存某些安全方面的标志，以实现快速匹配(如快速的策略匹配)等。

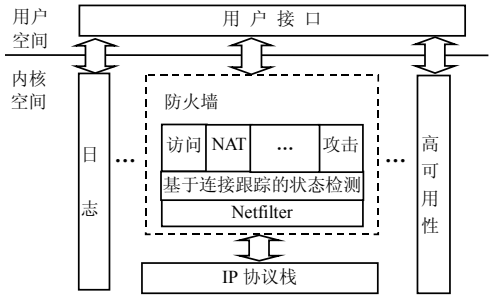

图1 基于Netfilter的防火墙基本框架

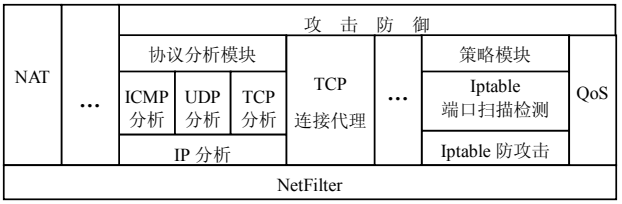

图2 攻击防御系统框架

2.2 攻击防御系统架构

图1中的攻击防御系统从内部又可以分为如图2所示的多个子模块。其中，协议分析模块负责对IP、ICMP、TCP、UDP等协议进行分析。某些网络攻击(如端口扫描)可以通过定制特定的策略来实现防御功能。图2中

用以支持防御策略的模块是策略模块。其中Iptable防攻击是防御策略模块，该模块以表的形式存放防御策略，此模块在Netfilter的FORWARD和LOCAL IN两个钩子处注册以使防御策略生效。端口扫描检测模块则是一个match模块，用以构成端口扫描检测策略。此模块主要应用时间分析机制实现对端口扫描的检测。例如：

iptables –t attack –A FORWARD –r/portscan –m psd –j DROP

2.3　攻击防御的动态过程

诸攻击防御模块都是基于Netfilter框架进行工作的。从Linux IP协议栈报文转发的动态过程来看，本文攻击防御系统工作在Netfilter的FORWARD和LOCAL_IN两个钩子上，如图3所示。在FORWARD处理过程中，还挂接了iptable_filter的处理操作；在LOCAL_IN钩子处，还有连接跟踪和iptable_filter的处理。在这两个钩子上，攻击防御系统是挂接在最后的，以确保防御模块的存在不会干扰其模块的工作。

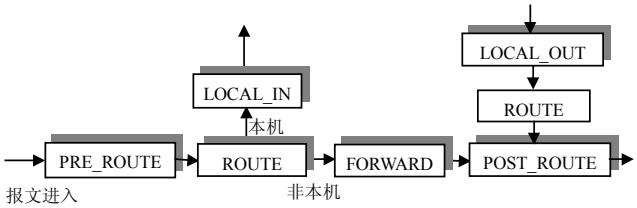

图3　攻击防御的动态过程

3　实验与分析

参照IDG Infoworld测试中心网络攻击测试基准IWSS16，本文将常见网络攻击分类进行了攻击测试。图4是简化的网络拓扑。其中，在PⅣ定制Linux操作系统的基础上构建了本文防火墙系统。攻击机170.1.1.1则是一台运行攻击测试包的PIII Linux PC。服务器150.1.1.1可以运行WEB、FTP等服务应用，模拟实际网络中的客户业务数据。攻击实验分为：

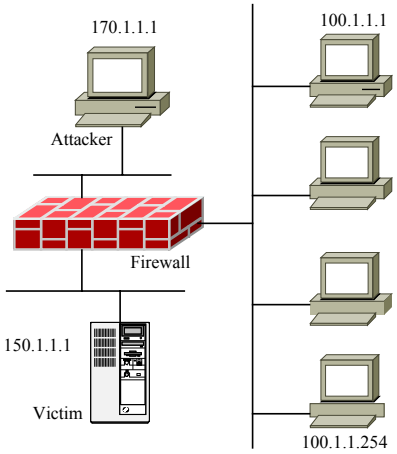

图4　网络攻击实验简化网络环境

3.1　防火墙本身攻击防御能力实验

攻击机向防火墙发起各种网络漏洞攻击，采取的典型攻击手段包括Ping of Death、LAND攻击、无确认FIN的TCP报文、无任何标志的TCP报文、SYN和FIN同时置位的报文、IP流选项报文、无效IP选项报文攻击等。启动防火墙上相应攻击防御子模块功能，观察防火墙自身防御能力的表现。实验结果表明，在攻击防御机制控制下，防火墙能够准确判断攻击行为，丢弃攻击报文，保证防火墙系统自身的正常工作。

3.2　保护服务器的抗攻击能力实验

攻击机通过防火墙向服务器发起各种网络漏洞攻击，打开或关闭防火墙上的相应攻击防御子模块功能，使用网络探针工具，观察攻击报文是否穿越防火墙，以及被保护主机是否受到攻击而崩溃。表1为几种典型攻击情况下服务器受保护情况的对比结果。实验结果表明，在攻击防御机制启用时服务器可避免受到攻击。

表1　攻击服务器对比实验结果

攻击类型	SYN碎片	UDPFlood	ICMPFlood	IP欺骗	每端口会话限制	端口扫描
启用防攻击时防火墙处理	丢弃	丢弃	丢弃	入口过滤检查	过滤超限报文	阻塞扫描源
未启用防攻击时防火墙处理	转发	转发	转发	转发	转发	转发

以上实验中，SYN碎片攻击的方法是，攻击机利用分片软件将TCP主动连接强行拆分成分片IP报文后，向服务器开启的444端口发起40分组/s的主动连接包。在未启动攻击防御功能时，该包被防火墙转发，使服务器出现DoS。启用攻击防御功能后，防火墙连接跟踪机制对缓存的分片进行分析，攻击报文被防火墙丢弃。

表2为端口扫描攻击实验的具体结果。在服务器上编写专门的测试用邮件接收服务进程，无任何安全防护，无会话限制。每次实验时服务进程端口随机变化。攻击机通过端口扫描方式以每进程每秒500端口的频率对此邮件服务器网段进行攻击。表2中端口扫描攻击防御模块门限参数(N，T)表示：T时间段(ms)内若攻击防御体系检测到同一主机访问了N个不同端口，则在该秒的剩余时间内，丢弃所有来自该攻击机的IP包。由此可知，增大攻击进程数并不能使攻击成功率显著提高。

实验结果表明，通过有效组合防火墙各子系统功能配置，本文攻击防御体系能够有效防御各种常见网络攻击，满足受信子网的安全需求。

3.3 保障正常业务通讯能力实验

攻击机向防火墙发起以耗尽防火墙资源为目的的大量网络攻击报文，判断防火墙在受到攻击而非常繁忙时，客户网段的业务访问情况。表3为在客户机100.1.1.1上运行FTP业务实验得到的结果。服务器150.1.1.1上启动FTP服务器进程，在攻击机170.1.1.1未发起攻击时客户机访问服务器的平均FTP流量为2 322 kB/s。从实验结果可以看出，由于FTP为基于TCP连接的业务，所以SYNFlood攻击对业务的影响最大。

表2 端口扫描攻击需要的平均试探时间 s

攻击进程	无防御	N=5 T=10	N=3 T=10
单进程	2 904	329 107	∞
10进程	453	109 166	∞

表3 防火墙启动攻击防御前后客户业务情况比较 kB/s

防攻击	SYNFlood	ICMP Flood	UDPFlood	碎片攻击
未启用	DoS	496	581	DoS
启用	1 398	2 272	2 140	2 308

4 结 束 语

本文提出的攻击防御的实施方案在Linux Netfilter架构上进行高强度的安全处理，在一个合理设计的攻击防御模块上提供了时间分析、协议分析、连接跟踪等基本攻击防御机制，能在通用Linux服务器上提供高强度的防火墙攻击防御服务，为企业局域网与拨号用户、域、网站、远程站点以及Intranet之间的通信提供强有力且灵活的保护。本文设计的防火墙攻击防御体系是一个通用的可扩展架构，具有操作简单、安全性高、抵御能力强、可扩展性好等优点，具有在现有架构上扩充支持IPv6协议族攻击防御的能力。由于Linux操作系统源代码是开放透明的，基于Linux操作系统架构的防火墙及其他网络安全产品正在成为一种趋势。

参 考 文 献

[1] Paulson, L D. Stopping intruders outside the gates[J]. IEEE Journal Computer, 2002, 35(11): 20-22

[2] 何海滨. 基于Linux包过滤的防火墙技术及应用[J]. 电子科技大学学报, 2004, 33(1): 75-78

[3] 颜学雄, 王清贤, 李梅林. SYN Flood攻击原理及预防方法[J]. 计算机应用, 2000, 20(8): 41-43

[4] Brockmeier J. Filtering packets with iptables[EB/OL]. http://www.netfilter.org, 2002-12-15

编 辑 刘文珍