第32卷 第16期 计 算 机 工 程 2006年8月
Vol.32 № 16 Computer Engineering August 2006
·安全技术· 文章编号：1000—3428(2006)16—0153—02 文献标识码：A 中图分类号：TP393.08

一种基于Linux的复合安全网关

杜 雨，李 涛，王丽辉，刘颖娜，杨 杰，王姝妲
（四川大学计算机系，成都 610065）

摘 要：通过对Linux内核和Netfilter框架的分析和研究，提出了一种集多种安全功能于一身的复合网关。该网关将防火墙、入侵检测和内容过滤3种安全功能用内核模块的形式实现，利用Netfilter框架的扩展功能，将各个安全模块加载进内核，从而在内核中实现对网络不同层次的安全功能的整合。

关键词：Netfilter；包过滤；入侵检测；内容过滤

A Hybrid Secure Gateway Based on Linux

DU Yu, LI Tao, WANG Lihui, LIU Yingna, YANG Jie, WANG Shuda
(Computer Department, Sichuan University, Chengdu 610065)

【Abstract】 By analyzing and studying the Linux kernel and Netfilter framework, This paper presents a hybrid gateway, which integrate multiple secure functions. The gateway implements the functions of firewall, intrusion detection system and content filtering as kernel modules and loads up these modules into kernel by utilizing the expansibility of Netfilter framework. Then the gateway implements the integration of different secure function at different layer of network.

【Key words】 Netfilter; Packet filtering; Intrusion detection; Content filtering

对于网络安全，在网络边界布置防火墙是个很好的解决办法，但传统的防火墙只能预防针对网络层的攻击，对实时的攻击无法响应，对基于内容的攻击更加无能为力[1]。这种基于单层次和静态防御的防火墙已难以满足网络与信息安全的需要。虽然市场上各种安全产品不断涌现，但各种不同的安全产品集中在一起工作时的协调性又成为另一个问题[2]，如何构建一个高效集成的网络环境已经成为一个迫切需要解决的问题。

1 系统总体结构

Linux2.4及以上内核中提供Netfilter框架来对数据包进行处理，Netfilter是一个抽象、通用化的框架，具有良好的扩展性能。图1中1、2、3、4和5分别表示Netfilter框架中定义5个HOOK点[4]，其中标号1为NF_IP_PRE_ROUTING点，标号2为NF_IP_LOCAL_IN点，标号3为NF_IP_ FORWARD点，标号4为NF_IP_POST_ROUTING点标号5为NF_IP_LOCAL_OUT点。数据包流经这些HOOK点时，如果有处理模块在该点注册，则调用该处理模块来对数据包进行处理。

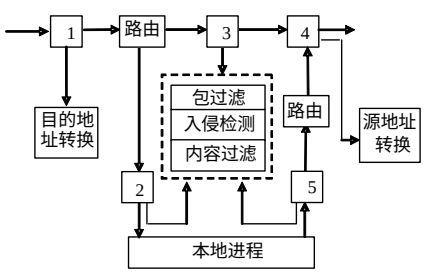

图1 各功能模块在Netfilter框架中的位置

LKBG需要在标号1和4点处插入防火墙地址转换功能模块，在2、3和4点处插入实现防火墙包过滤、入侵检测和内容过滤的功能模块（见图1）。

以HOOK点2为例，数据包到达HOOK点2后，首先要通过防火墙包过滤模块及状态检测的过滤；然后数据包到达入侵检测模块，入侵检测模块对数据包进行过滤，检查数据包是否为攻击数据包；通过入侵检测后，最后数据包到达内容过滤模块，数据包在这里将进行会话的还原，然后对还原后的数据流进行过滤。

2 系统实现

2.1 防火墙模块的实现

通过对Netfilter框架的深入分析，LKBG防火墙模块设计分为过滤模块、状态检测模块、地址转换模块。

包过滤模块是对数据包的源/目的IP地址、源/目的端口、输入/输出接口等进行检测。其实现思想是：在HOOK点处注册过滤函数，该函数建立过滤规则链表，链表的每个节点就是条规则。这些规则主要是对数据包的TCP层和IP层协议头中的信息进行匹配（match）以及规定匹配后的目标（target）。数据包到达包过滤模块后，过滤函数遍历对应链表上的规则（节点），根据数据包与规则之间的匹配状况来决定数据包的目标。如果匹配规则，则由包过滤函数返回NF_ACCEPT给nf_hook_slow，nf_hook_slow随后将调用入侵检测函数来对数据包进行处理；如果不匹配，则返回NF_ACCEPT，通知内核释放该数据包。另外，在包过滤模块还有一个接收入侵检测警报信息的函数，该函数根据入侵检

基金项目：国家自然科学基金资助项目（60373110）；教育部博士点基金资助项目（20030610003）；四川大学创新基金资助项目
作者简介：杜 雨(1981—)，男，硕士生，主研方向：网络安全，人工智能；李 涛，博导、教授；王丽辉、刘颖娜、杨 杰、王姝妲，硕士生
收稿日期：2005-10-10 **E-mail：**duyu210@sina.com

测模块发来的警报信息，生成相应的过滤规则来阻止攻击。

状态检测模块是对TCP连接的完整的会话过程的跟踪记录。其实现思想是：首先建立一个会话连接状态检测表（以下简称状态检测表），当内核接收到一个初始化 TCP 连接的 SYN 包时，这个带有 SYN 的数据包被防火墙的规则链表检查。该包在规则链表里依次序比较。如果在检查了所有的规则后，该包都没有被接收，那么返回 NF_DROP，并将一个 RST 的数据包发送到远端的机器。如果该包被接收，那么本次会话被记录到状态检测表里。随后的数据包(没有带有 SYN 标志)就和该状态检测表的内容进行比较。如果会话是在状态表内，而且该数据包是会话的一部分，该数据包被接收，并返回 NF_ACCEPT。如果不是会话的一部分，该数据包被丢弃，返回 NF_DROP。这种方式提高了系统的性能，因为每一个数据包不是和规则链表比较，而是和状态检测表比较。实际上，该状态检测表由状态检测、入侵检测和内容过滤模块共同维护，状态检测模块只是对连接状态表进行初始化记录，而后入侵检测和内容过滤模块再根据自己的检测结果来对该表进行更新，以决定是否接受后继的数据包。

地址转换模块主要是实现对 IP 地址的伪装、转换和服务端口的转换和重定向。在 HOOK 点 1 处是对接收到的数据包将其地址信息和端口信息改写为规则链表中规则指定的目的地址，再进行下一步处理；而在 HOOK 点 4 处是对待发送出去的数据包修改其源地址和端口信息后再将它发送到路由。

2.2 入侵检测模块的实现

根据通用入侵检测模型(Common Intrusion Detection Framework, CIDF)的框架设计，一个完善的入侵检测系统应该由以下几个模块组成：事件产生模块，事件分析模块，事件响应模块和规则库。由于本网关入侵检测的数据采集是利用Netfilter框架上流动的数据包，因此就省略了事件产生模块的设计。实际上，这避免了通常的IDS单独抓取数据包造成系统开销过多的缺点，对已获得的数据包进行了最大程度的利用。入侵检测模块主要由以下几个功能模块组成：事件分析模块，事件响应模块和规则库文件[2]和联动模块。

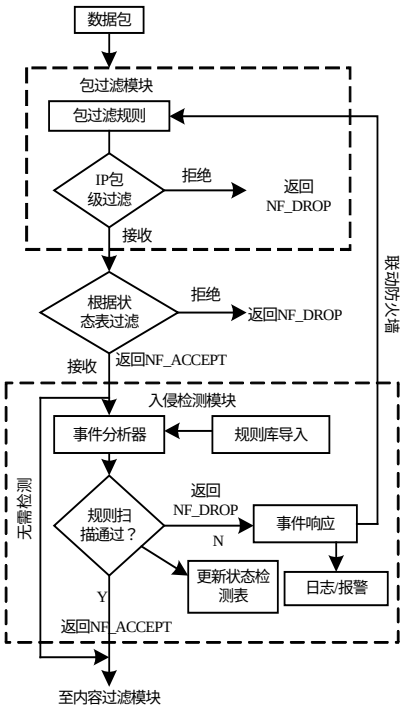

图 2 包过滤和入侵检测模块的工作流程

在本网关的设计中，将 IDS 模块放在包过滤模块之后，直接使用通过内核并经过防火墙模块过滤后的数据包。当数据包通过防火墙过滤再交由入侵检测模块处理时，入侵检测模块对数据包的处理量已经大大减少了，这在一定程度上提高了网关处理数据包的效率。当防火墙模块对数据包进行过滤并返回 NF_ACCEPT 给 nf_hook_slow 后，nf_hook_slow 就调用入侵检测处理的函数对数据包进行处理。入侵检测模块的框架和对数据包的处理流程如图 2 所示。

数据包通过防火墙过滤后，直接转交给入侵检测模块的事件分析器。之前需要由用户空间将规则库文件导入，在内存中构建检测规则的链表。然后由事件分析器将数据包遍历检测规则链表来进行匹配。如果检测通过，则继续发送给内容过滤模块处理，同时更新状态检测表，决定当前连接的后继数据包都被接收，下一步不再需要进行入侵检测；如果检测未通过，即检测到攻击，则返回 NF_DROP，释放该数据包，同时事件响应模块对该次扫描进行日志记录和报警，然后更新状态表，以阻止后续数据包的接收，并将该报警信息通知防火墙包过滤模块。

由于 CIDF 模型中并未提供 IDS 和防火墙协同工作的模型，因此根据实际的需要，我们在该模型的基础上增加了 IDS 与防火墙联动的模块。该模块是根据事件响应模块产生的报警信息，按照预定的协议格式，将报警信息发送给防火墙包过滤模块，防火墙包过滤模块接收到报警信息后再将这些规则信息组合成防火墙规则添加到包过滤规则队列中。联动模块同时将内存中已经建立的规则链表进行更新，将与通知防火墙的报警信息重复的规则从该链表中去掉，这样可以减少对后续数据包匹配规则的数量。

2.3 内容过滤模块的实现

在内容过滤模块的实现中，过滤对象是一个完整会话中的所有的数据包，而不是单个的数据包。如果状态检测表指示无须对数据包进行过滤，则直接转发，如视频和音频数据；如果状态检测表要求对数据包进行应用层检测，则将这些关联的数据包放入模拟出的 TCP 协议栈中的缓冲区中，将包含分散的数据内容的数据包队列在缓冲区中还原成一个完整的数据流，再对还原后的数据流进行过滤，最后再将缓冲区中的数据包继续沿 Netfilter 框架发送出去。内容过滤模块的工作流程如图 3 所示。内容过滤模块主要分为 3 个功能模块：还原模块，过滤模块和发送模块。

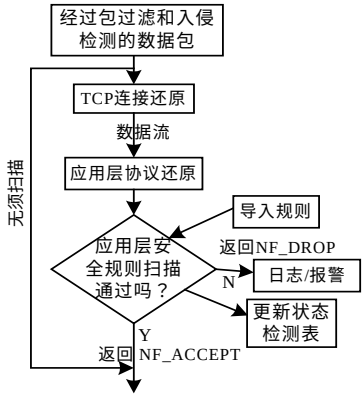

图 3 内容过滤模块工作流程

还原模块的主要功能是负责在 IP 层实现 TCP 层会话还原功能。其实现思想是：把一个 TCP 连接视为一个对象，复用防火墙状态检测模块建立的状态检测表，使用它为会话过

(下转第 176 页)