基于 Netfilter 技术的内容过滤技术研究与实现①

Research and Implementation of the content – inspection Based on Netfilter

周 诚 （中南大学 信息科学与工程学院 湖南长沙 410075）

摘要：随着网络的迅猛发展，网络安全问题显得日益重要，其中防火墙技术的研究是网络安全领域的重要研究课题。基于 Netfilter 技术的内容检测技术研究是实现复合防火墙系统的重要步骤，其意义在于：采用内容检测技术能对报文进行更仔细的检测，是传统包过滤的重要补充，从而最大限度的保证网络的安全。该技术的研究与应用是一个有着重要实用价值的研究课题，在网络安全领域具有广泛的应用前景。

关键词：网络安全 防火墙 Netfilter 内容过滤

1 Netfilter 框架概述[1-3]

Linux 内核防火墙底层结构采用的 Netfilter 框架，该框架是一个新型的分析处理特定协议数据包的框架，是嵌入内核 IP 协议堆栈的一系列调用入口（也称为内核空间，kernel space），如图 1。

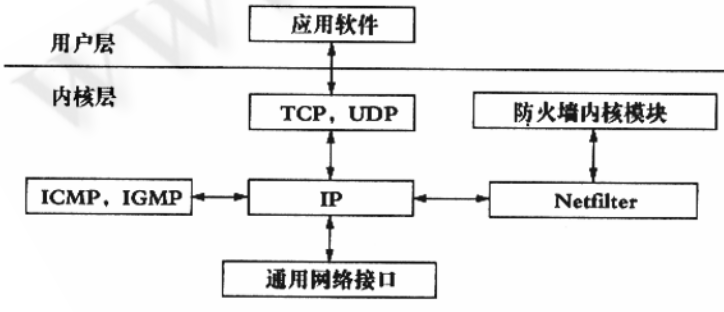

图 1 Netfilter 框架在 Linux 内核中的位置

在内核中通过 Netfilter 结构将防火墙对数据包的处理引入到了 IP 层中实现，防火墙的代码与实现 IP 的代码完全分离，从而构成不同的模块，使得防火墙修改和扩充变得容易。Netfilter 框架是不同于通常的 Berkerley 套接字接口的协议数据包处理框架，它在多种协议的处理过程中提供了一套类似的检查点（钩子，HOOK）。

按照报文来源和去向，分为三类：流入的、流经的和流出的。其中流入和流经的报文需要经过路由才能区分，而流经和流出的报文则需要经过投递，此外流经的报文还有一个 FORWARD 的过程，即从一个 NIC 转到另一个 NIC（转发）。

如图 2，Netfilter 根据报文的流向，设置了五个 HOOK，如下：NF_IP_PRE_ROUTING，在刚刚进入网络层的包在此完成版本号、校验和等检测；NF_IP_FORWARD，要转发的包在此进行检查；NF_IP_POST_ROUTING，对马上要通过本地的包在此进行检查；NF_IP_LOCAL_IN，对经过路由查找后要送往本机的包在此进行检查；NF_IP_LOCAL_OUT，对本机发出的包在此进行检查。每个注册的钩子经过处理后都会有个返回值，告知 Netfilter 核心代码处理结果，以便对报文采取相应的动作，继续或丢弃等处理。每个注册的钩子函数经过处理后都会有个返回值，告知 Netfilter 核心代码处理结果，以便对报文采取相应的动作，如 NF_ACCEPT，继续正常的报文处理；NF_DROP，将报文丢弃。

当开发防火墙时，要用到防火墙模块的 HOOK 注册函数和注销函数。注册一个 Netfilter 的钩子函数需要调用 nf_register_hook 函数，注销 Netfilter HOOK 则需要调用 nf_unregister_hook 函数。

2 内容检测技术工作原理与实现

2.1 内容检测技术的工作原理

内容检测技术的工作原理就是利用 Netfilter 的钩子函数在网络层中作用，在相应的位置加载检测程序，以实现在网络层对转发包通过采用的匹配算法进行指定内容的检测。

① 湖南省自然科学基金项目（编号：02JJY2094）资助

由于这里主要是研究内容检测技术在防火墙中的应用，因此根据防火墙的特点：防火墙充当内网和外网的接口，防火墙本身发出的包或进入防火墙的包占所有通过防火墙的包的比例很小，为了突出防火墙的性能，因此内容检测技术要检测的数据包重点针对转发的数据包，而不是以防火墙本身为源或以防火墙本身为目的数据包。

通过 skb_buff 中的数据指针和数据区的大小变量就可以找到包中数据区的起始位置和包的大小，然后就可以开始进行匹配查找。

2.2 内容检测系统的设计

在防火墙系统中，主要采用内容检测技术的部分，组成了内容检测系统，下面将进一步描述内容检测系统的设计及实现过程。

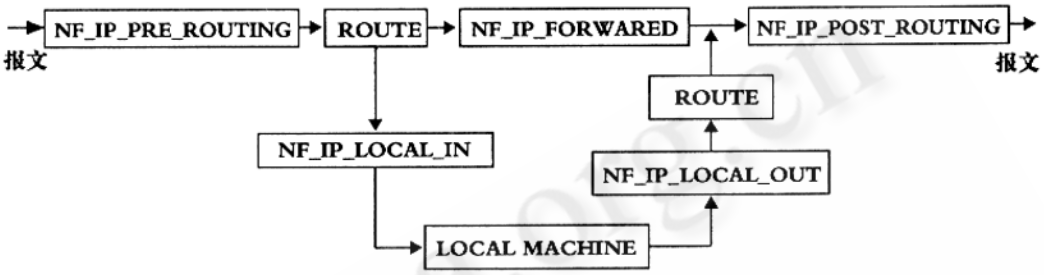

图 2　Netfilter 框架中的 HOOK

如图 2，在 Netfilter 架构中可以知道 NF_IP_PRE_ROUTING、NF_IP_POST_ROUTING、NF_IP_FORWARD 是用来控制数据包的转发。由于 NF_IP_PRE_ROUTING 钩子存在以防火墙本身为目的的数据包经过，NF_IP_POST_ROUTING 也存在以防火墙本身为源的数据包经过，只有 NF_IP_FORWARD 处经过的数据包才是完完全全的是转发数据包，而且所有转发的数据包都要经过这里。而钩子 NF_IP_PRE_ROUTING、NF_IP_POST_ROUTING 处还有包过滤系统存在，同时考虑到本防火墙中地址转发是利用的 nat 表来实现的（如图 2，nat 表是在 POSTROUTING 链处实现的 SNAT，在 PREROUTING 链处实现的 DNAT 的）[1]。

为了减少对不必要的数据包检测，从网络安全的层次上考虑，因此选择 NF_IP_FORWARD 作为内容检测系统的加载钩子，就可以对所有转发的数据包都进行检测。对于网络数据包中的数据检测，对 IP 协议中的数据检测具有代表性，因此防火墙系统主要针对 IP 协议的数据包进行检测。

当确定 HOOK 的位置，下一步就是寻找检测算法，这里以 BM 改进算法作为检测的算法。这里采用了套接字缓冲区（skb_buff）[3] 的数据结构。套接字缓冲区是网络部分重要的数据结构，描述内存中的一个数据区域，存放网络传输的数据包。在整个网络传输中，套接字缓冲区作为数据的载体，保证了数据的可靠和稳定，而且网络部分的各层都和该数据结构密切相关。因此如果 Netfilter 框架要对网络数据包进行处理，就必须依靠套接字缓冲区。

（1）构造 HOOK 钩子的注册函数，并将钩子函数注册到 NF_IP_FORWARD 钩子上面，当本模块加载后，内容检测子系统就开赛监控所有转发的数据包，如图 3 的左边部分。

（2）钩子函数的实现算法如图 3 的右边部分，当一个 IPV4 数据包经过 NF_IP_FORWARD 时候，就会触发该函数，进入钩子函数进行检测。

（3）当系统卸载本模块的时候，调用模块清除函数，卸载钩子函数

如图 3，当有转发的数据包经过 NF_IP_FORWARD 钩子时，就会被内容检测系统拦截：首先，判断是否为 IP 数据包，如果不是则直接返回，如果是则进入真正的内容检测环节。通过 sk_buff 数据结构的指针得到报文数据的指针和报文大小，然后调用模式匹配模块开始进行匹配。当匹配结束的时候，根据结果判断是否匹配：是，说明该报文满足条件，丢弃；不是，则修改匹配字符串指针，得到下一个匹配字符串，重新进行匹配测试。当所有的匹配规则结束，则结束匹配检测，退出内容检测系统，等待下一次数据包的到来。

3　性能分析及测试

3.1 与代理服务的内容检测系统的比较

内容检测系统在代理服务中也存在（简称 A 系统），但与这里的内容检测系统（简称 B 系统）还是有很大区别的：

首先，A 系统是基于代理的，而代理是工作在应用层，因此 A 系统也是工作在应用层的；而 B 系统是基于内核的钩子，而钩子是在网络层中通过嵌入实现的，因此 B 系统主要工作在网络层。

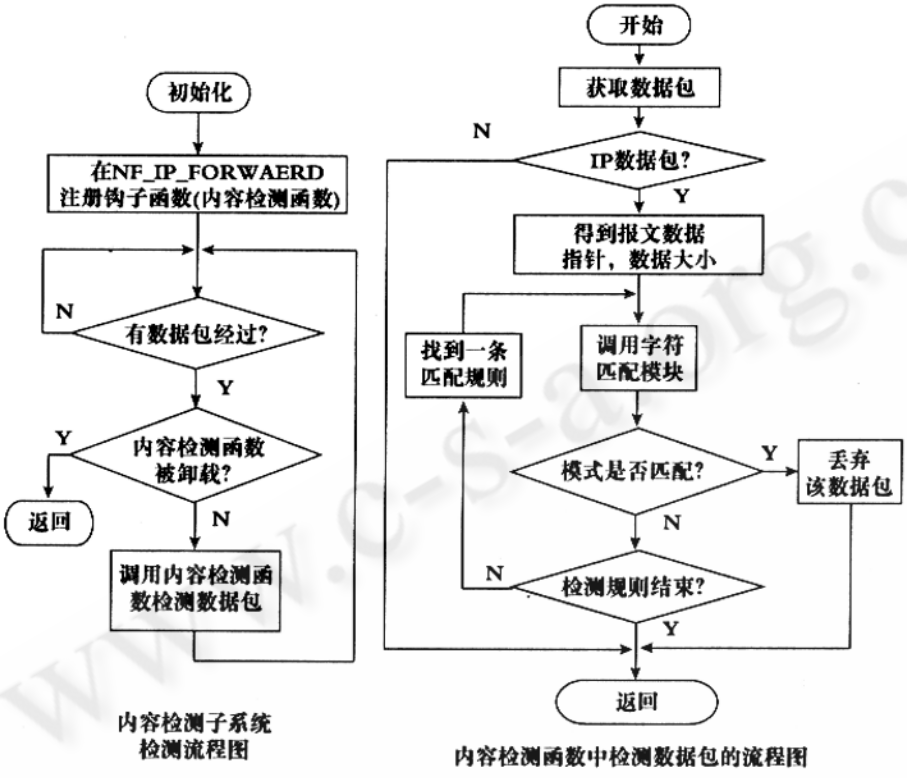

图 3　内容检测系统原理图

其次，由于代理的特点，对于不同的服务要用不同的代理，也就是说，要实现对不同服务的内容检测，则要使用不同的 A 系统，适应性差。而从网络层来看，不同的服务并没带来很大差别，内核的钩子依然会拦截获该数据包进行检测，也就是说 B 系统能完成预期的检测，而不需要重新再构造一个新的系统。因此 B 系统的适应性要强于 A 系统。

但 A 系统也有自己的特点，比如说现在 A 系统的日志功能已经很强大了，而 B 系统由于工作在内核，因此其日志功能相对于 A 而言则要差些。

而且根据设计要求，当数据包中有匹配字符串时，则该数据包将被丢弃，则就要求选择合适的匹配字符串，这又是一个相当复杂的问题：如何得到合适的匹配字符串，制定匹配规则库。

3.2 系统测试

内容检测主要是针对报文中带有固定信息进行检测，以防止该信息通过防火墙。由于内容检测系统中的内容检测技术，是采用 Netfilter 与系统的网络层紧密相连，因此可以检测每个包中的报文信息，因此当带有固定信息通过防火墙时，将会发出报警，并按照内容检测系统的设定进行处理。

比如：IIS 蠕虫会通过 80 端口对 Unix Web 服务器进行大量的对 cmd. exe 的请求，也就是说报文中含有“cmd. exe”字符串。如果指定该字符为内容检测的信息，则含有该字符串的报文都将引起报警。

4　总结与展望

本文通过提出的基于 Netfilter 技术的内容检测技术的实现虽然可以使防火墙系统在功能、安全性得到较大程度的改进，但随着时代的发展，网络安全问题还是会更加突出。

目前新一代安全产品的应用不断普及，新的技术不断引入，随之而来的网络安全产品的融合、协同越来越引起人们的关注，也成为网络安全重要的发展方向。如何更好把多种安全技术应用到防火墙系统中，也使得防火墙研究得到前所未有的发展机遇与挑战。

参考文献

1 Rusty R. Linux 2. 4 Packet Filtering HOWTO [Z], mailing list netfilter@ lists. samba. org ? v1. 0. 1 , CST, 2000.

2 Russell PR. Writing a Module for netfilter[J]. Linux Magazine, 2000. http://www. linux – mag. com/2000 – 06/gear_01. html

3 毛德操、胡希明，Linux 内核源代码情景分析[M]. 杭州：浙大出版社，2001，9.

4 姚晓宇等，Linux 内核防火墙 Netfilter 实现与应用研究[J]，计算机工程，2003，5.

5 周诚等，一种基于 Netfilter 的认证方法研究与实现[J]，计算机测量与控制，2005，4（13）.

6 周诚，基于 Netfilter 技术的复合防火墙系统研究与实现[J]，计算机测量与控制，2007，6.