Linux内核中的防火墙

华中师范大学　王莉 黄光明

Linux由于其开放源代码的特性，近年来得到了迅速的发展。作为一个高性能的网络操作系统，Linux内核中的防火墙扮演着非常重要的角色。

Linux防火墙底层结构分析

Netfilter简介

Netfilter是Linux2.4内核中，用于扩展各种网络服务的结构化底层框架，比以前任何一版Linux内核的防火墙系统都要完善。Netfilter提供了一个抽象、通用化的框架，该框架定义的一个子功能的实现就是包过滤子系统。

Netfilter框架包含以下三部分：

1.为每种网络协议(IPv4、IPv6等)定义了一套钩子函数，这些钩子函数在数据包流过协议栈的几个关键点时被调用。在这几个点中，协议栈把数据包及钩子函数标号作为参数，调用Netfilter框架。

2.内核的任何模块可以对每种协议的一个或多个钩子进行注册，实现挂接。这样当某个数据包被传递给Netfilter框架时，内核能够检测出是否有模块对该协议和钩子函数进行了注册。如果注册了，就调用该模块注册时使用的回调函数，这样这些模块就有机会检查该数据包、丢弃该数据包或是指示Netfilter将该数据包传入用户空间的队列。

3.排队的数据包传递给用户空间后，被异步处理。一个用户进程能检查数据包，修改数据包，甚至可以重新将该数据包通过离开内核的同一个钩子函数中注入到内核中。

Netfilter在IPv4中的结构

一个数据包按照如图1所示的过程通过Netfilter系统：

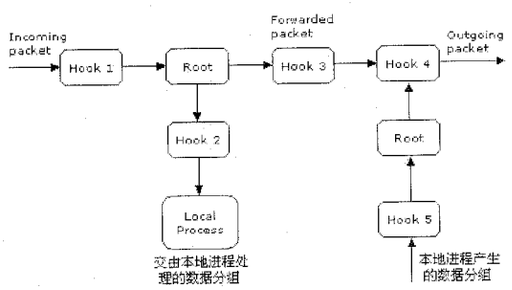

图1 Netfilter结构图

从图中可以看到，IPv4一共有5个钩子函数，分别为：NF_IP_PRE_ROUTING、NF_IP_LOCAL_IN、NF_IP_FORWARD、NF_IP_POST_ROUTING、NF_IP_LOCAL_OUT。

数据包进入系统后，有3种可能的流程：

1.NF_IP_PRE_ROUTING->NF_IP_FORWARD->NF_IP_POST_ROUTING

主机接收到需要它转发的数据包后，首先经过插入点1，如果没有任何插入函数的话，系统将做出路由决定，决定该数据包的走向。然后数据包会经过3、4号插入点，离开系统并被发送到网络上。

2.NF_IP_PRE_ROUTING->NF_IP_LOCAL_IN

主机接收到发往本地的IP数据包后，首先经过插入点1，系统做出路由决定，决定把该数据包发往本地，数据包经过插入点2后被应用程序所接收。

3.NF_IP_LOCAL_OUT->NF_IP_POST_ROUTING

当本地产生数据包时，该数据包首先经过插入点5，数据包经过插入点4后被转发到网络中。

iptables

在Linux2.4内核中，一个基于Netfilter框架的数据包选择系统被应用，它就是iptables。

Netfilter有三种工作模式：包过滤模式(packet filtering)、网络地址转换模式(NAT)和报文修改模式(packet mangling)。每种工作模式都在各个插入点上制定一类IP数据包处理规则，每一类规则都自成一个IP规则表。

在Netfilter结构中，使用的三个表是filter、nat、mangle，分别对应这三种工作模式。这三个规则表互不干扰，独立执行。与内核2.2相似的是，可以在用户态使用命令在这些链中插入规则，不过2.2使用的是ipchains命令，而2.4使用的是iptables命令。

iptables作为模块，称为iptables_filter.o，它可以在第一次运行iptables时被自动装载，也可以永久性地编译到内核中。

防火墙配置实例

非军事区(DMZ)

非军事区是一段网络，它允许Internet的流量出入Intranet，同时仍能保证Intranet的安全。也就是说，DMZ(Demilitary Zone)提供了在Internet和Intranet之间的缓冲。

DMZ通过使用服务器和第三层设备，防止将Intranet直接暴露给Internet，从而提高了安全性，是构建防火墙基础设施最普遍的安全模式。实践中，通常将那些为安全性较差的网

络提供服务的服务器，放置在单独的网段内，通过防御主机过滤进入非军事区的各种类型封包，以完成有限的保护。

这里，就使用iptables工具配置一个具有DMZ的防火墙。

物理网络

如图2所示，局域网的公共网络地址为202.114.36.185。DMZ区和Intranet均为私有地址，地址空间分别为192.168.0.0/24和192.168.1.0/24。

在一台主机上安装3块网卡eth0、eth1和eth2。eth0为外部网络接口，eth1为DMZ区网络接口，eth2为Intranet网络接口。给eth0网卡分配一个公共网络地址202.114.36.185，用来与Internet相连;给eth1网卡分配私有地址192.168.0.2，用来与DMZ区相连;给eth2网卡分配私有地址192.168.1.2，用来与Intranet相连。

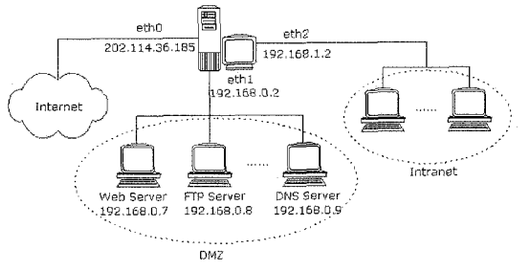

图2 Linux防火墙拓扑图

防火墙配置

用户需要以root身份登录，来使用iptables工具。进入系统以后，可以先通过命令“iptables -L”来察看当前设定的防火墙规则，如果希望了解防火墙设置的详细信息，可以使用“iptables -list”命令来查看。

清除所有链的规则

清除一个链中所有规则的简单方法，是使用‘-F’或‘--flush’命令。如果不指定链的话，所有链都将被清空。所以，这里的命令是:

```
iptables -F
```

设定初始规则

清除了所有链的规则之后，接下来就是要设定初始规则。所谓的初始规则是指“当到达的数据包不在你的规则之内时，该包是否可以通过防火墙，以这些规则的设定为准”。这里，我们采用禁止一切的默认策略，即:

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

建立状态数据包检查功能

```
iptables -A INPUT -m -state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m -state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FOWARD -m -state --state ESTABLISHED,RELATED -j ACCEPT
iptables -t -nat -A PREROUTING -m -state --state ESTABLISHED,RELATED -j ACCEPT
iptables -t -nat -A POSTROUTING -m -state --state ESTABLISHED,RELATED -j ACCEPT
```

防止IP欺骗

```
iptables -t nat -A PREROUTING -i eth0 -s 192.168.0.0/24 -j DROP
iptables -t nat -A PREROUTING -i eth0 -s 192.168.1.0/24 -j DROP
```

区域之间规则设定

1)进行源地址转换:

```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 202.114.36.185
```

2)Internet和Intranet之间

拒绝外部网络对内部网络的所有直接访问:

```
iptables -t nat -A PREROUTING -d 192.168.1.0/24 -i eth0 -j DROP
```

3)DMZ和Intranet之间

允许内部网络对DMZ的访问:

```
iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.0.0/24 -i eth1 -j ACCETP
```

允许DMZ对内部网络的如下访问:

```
iptables -A FORWARD -p tcp -s 192.168.0.0/24 --sport 80 -d 192.168.1.0/24 -i eth2 -j ACCEPT
iptables -A FORWARD -p udp -s 192.168.0.0/24 --sport 53 -d 192.168.1.0/24 -i eth2 -j ACCEPT
```

4)DMZ和Internet之间

拒绝外部网络对DMZ的直接访问:

```
iptables -t nat -A PREROUTING -d 192.168.0.0/24 -i eth0 -j DROP
```

提供Web服务:

```
iptables -t nat -A PREROUTING -p tcp -d 202.114.36.187 --dport 80 -i eth0 -j DNAT --to 192.168.0.7
iptables -A FORWARD -p tcp -d 192.168.0.7 --dprot 80 -i eth1 -o eth0 -j ACCEPT
```

提供FTP服务:

```
iptables -t nat -A PREROUTING -p tcp -d 202.114.36.188 --dport 21 -i eth0 -j DNAT --to 192.168.0.8
iptables -A FORWARD -p tcp -d 192.168.0.8 --dprot 21 -i eth1 -o eth0 -j ACCEPT
iptables -A FORWARD -p tcp -s 192.168.0.8 --sprot 20 -i eth0 -o eth1 -j ACCEPT
```

允许域名解析:

```
iptables -t nat -A PREROUTING -p udp -d 202.114.36.189 --dport 53 -i eth0 -j DNAT --to 192.168.0.9
iptables -A FORWARD -p udp -d 192.168.0.9 --dprot 53 -i eth1 -o eth0 -j ACCEPT
iptables -A FORWARD -p udp -s 192.168.0.9 --sprot 53 -i eth0 -o eth1 -j ACCEPT
```

通过以上各步骤的配置，建立了一个简单的具有DMZ的防火墙。当然，需要将规则保存到/etc/rc.d/rc.firewall文件中，并用chmod赋予该文件执行权限。还需要在/etc/rc.d/rc.local中加入一行sh/etc/rc.d/rc.firewall，这样当系统启动时，这些规则将自动生效。

防火墙作为目前用来实现网络安全的一种主要手段，主要用来拒绝未经授权用户的访问，阻止未经授权用户存取敏感数据，同时允许合法用户可以不受妨碍地访问网络资源。用Linux做防火墙是一个非常经济的方案，无需任何高档的设备就可以实现。正是由于它的高效、经济与免费等特性，使它受到了越来越多用户的青睐。