第27卷 第3期
2005年9月

西 北 地 震 学 报
NORTHWESTERN SEISMOLOGICAL JOURNAL

Vol. 27 No. 3
Sept., 2005

应用 Netfilter/iptables 构建甘肃地震信息网络安全防火墙系统

郝 臻[1]，梁子斌[1]，郝 柽[1]，马占虎[2]，李少华[1]

(1. 甘肃省地震局，甘肃 兰州 730000；2. 中国地震局预测研究所兰州科技创新基地，甘肃 兰州 730000)

摘 要：介绍了应用 netfilter/iptables 技术构建甘肃地震信息网络安全防火墙的技术方案和设计思想。较完整地给出了甘肃地震信息网的防火墙配置脚本，并对每个功能的实现策略作了详尽的解释。客观地分析了 netfilter/iptables 技术的优点和不足。

关键词：甘肃地震信息网；防火墙；包过滤；Netfilter/Iptables；DMZ；NAT

中图分类号：TP393.08 文献标识码：B 文章编号：1000－0844(2005)03－0272－06

Building Security Firewall System of Gansu Seismic Information Network Relies on Netfilter/iptables Technology

HAO Zhen[1], LIANG Zi-bin[1], HAO Cheng[1], MA Zhan-hu[2], LI Shao-hua[1]

(1. *Earthquake Administration of Gansu Province, Lanzhou 730000, China*;
2. *Lanzhou Base of Institute of Earthquake Prediction, CEA, Lanzhou 730000, China*)

Abstract: The technological scheme and design method of building Security Firewall of Gansu Seismic Information Network through Netfilter/iptables techniques are introduced. The firewall disposition script of this system is completely showed, and the implementation strategy of every function is detailedly explained. Finally, the advantages and disvantages of netfilter/iptables techniques are objectively analyzed.

Key words: **Gansu Seismic Information Network; Firewall; Packet Filtering; Netfilter/Iptables; DMZ; NAT**

0 引言

随着互联网技术的发展和应用，网络安全变得至关重要。Firewall(防火墙)是加强企业或政府机构内部网络安全防范的一个非常重要的部分，它是设置在被保护网络和外部网络之间的一道屏障，来自和发往互联网的所有信息都必须由防火墙出入，防火墙只允许授权信息通过，本身不能渗透。防火墙可以确定哪些内部服务允许外部访问，哪些外部服务可由内部人员访问。防火墙采用先进的信息安全技术，是集安全访问控制、流量统计控制、安全审计、用户验证、网络管理于一身的网络安全解决方案。

然而，专业的防火墙产品价格昂贵，配置管理复杂，一般的中小企业和事业单位由于受财力、技术实力的局限往往不易采用。Netfilter/iptables 是 Linux 操作系统内置的防火墙解决方案，它功能强大、配置容易，更得益于 Linux 操作系统的健壮性和可靠性以及几乎无限范围的可定制性，在业界享誉很高。Netfilter/iptables 是免费的，是中小企业防火墙解决方案的最佳选择。

1 包过滤技术及 Netfilter/iptables 简介

收稿日期：2004-12-21
基金项目："十五"项目：甘肃省地震信息服务系统建设；中国地震局兰州地震研究所论著编号：LC20050034
作者简介：郝臻(1970－)，男(汉族)，甘肃平凉人，工程师，现主要从事甘肃省地震信息网络系统的建设、管理与开发.

包过滤(Packet Filtering)技术是指通过检查所流经的数据包的包头(IP 头、TCP 头、UDP 头),从而决定整个数据包的命运。它可能会决定杀死这个包,也可能会接受这个包(让这个包通过),或者执行其它更复杂的动作。包过滤技术通常检查的包头信息主要有:数据包源地址、数据包目的地址、通信协议、数据包源端口、数据包目的端口、TCP 包头中的 ACK 位、ICMP 消息类型等。

Netfilter/iptables 是 Linux 平台下的一个功能强大的 IP 信息包过滤工具。在 Linux 2.4 及其以上版本的内核中,Netfilter/iptables 代替了原 2.2 版中的 ipChains 包过滤工具。它是一个全新的包过滤解决方案,功能十分强大,用户更容易理解,更容易配置和使用。Netfilter/iptables 工作在网络层,通过检查数据包的 IP 头、TCP 头或 UDP 头来实现数据包过滤,其过滤流程如图 1 所示。

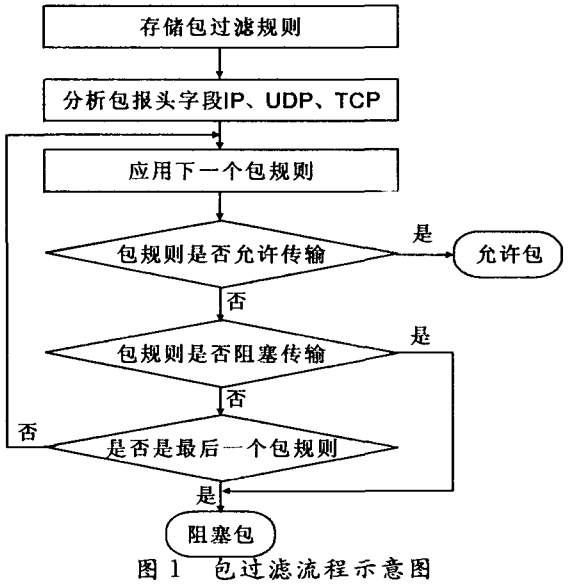

图 1　包过滤流程示意图

Fig. 1　Flow chart of Packet Filtering.

Netfilter/iptables 是两层结构,其中 iptables 只是一个管理内核 IP 包过滤的工具,它为用户配置防火墙提供了方便。iptables 可以添加、修改、删除内核包过滤表中的规则,其过滤功能是由内核模块 Netfilter 及其相关模块完成的。Netfilter/iptables 系统的主要功能有:状态包过滤、网络地址翻译(转换)。其主要用途是建立互联网防火墙和基于状态的包过滤,用 NAT 或地址伪装带动局域网上网,用 NAT 实现透明代理,通过修改 IP 包的 Tos 字段实现更复杂的功能。

2　Netfilter/iptables 的总体结构及工作原理

Netfilter/iptables 的总体结构如图 2 所示,其内核空间(netfilter 组件)由三种类型的表(table)组成:它们分别是 filter 表、mangle 表和 nat 表;其中每个表又由一些链(chain)组成。规则(rule)被分组放在链中。即 netfilter 是表的容器,表是链的容器,链是规则的容器。

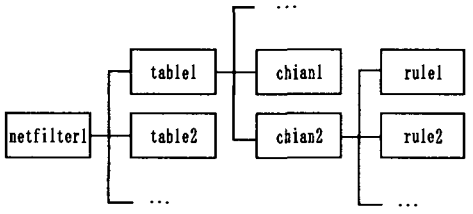

图 2　netfilter 的总体结构示意图

Fig. 2　Integrated structural chart of netfilter.

在 filter 表中,系统预定义了三种默认链:INPUT、OUTPUT 和 FORWARD;在 nat 表中,系统同样预定义了三种默认链:PREROUTING、OUTPUT、POSTROUTING;而在 mangle 表中,系统则预定义了五种默认链:INPUT、OUTPUT、FORWARD、PREROUTING 和 POSTROUTING;并且,在这三种表中,用户均可以定义自己的链。

Netfilter/iptables 的工作原理:

(1)用户使用 iptables 命令在用户空间(iptables 组件)设置过滤规则,并存储在内核空间的信息包过滤表中。这些规则告诉内核对经过防火墙的信息包作那些处理:ACCEPT(放行)、DROP(阻塞)或 REJECT(丢弃)。

(2)内核空间接管过滤工作,对入站的信息包进行路由并过滤,其过程如图 3 所示。

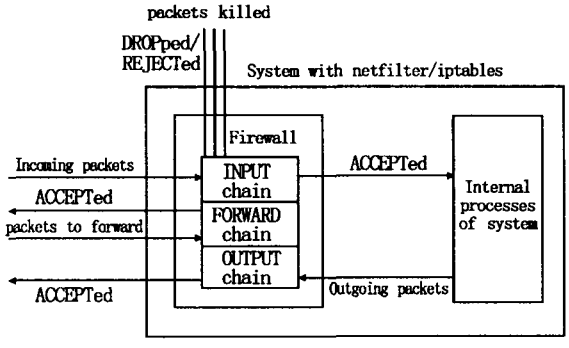

图 3　netfilter 数据包过滤过程

Fig. 3　Filter process of netfilter data packet.

由图 3 可以看出:对来自外部、且目的地址是本地系统的数据包,防火墙内核空间将它传递到 filter 表的 INPUT 链,Netfilter 按照用户设定的过滤规则对数据包进行过滤;如果数据包源自外部系统,且

目的地址也是外部系统，那么内核将它传递到 filter 表的 FORWARD 链；如果数据包源自本地系统，并且数据包的目的地址是外部系统，内核将它传递到 filter 表的 OUTPUT 链。

当入站的信息包与某条规则匹配，那么内核就对该信息包执行由该规则的目标制定的操作，如果目标为 ACCEPT，则允许该信息包通过，并将该包发给相应的本地进程处理。如果目标为 DROP 或 REJECT，则不允许该信息包通过，并将该包阻塞并杀死。如果信息包与链中的任何规则都不匹配，那么内核将参考该链的策略来决定如何处理该信息包。

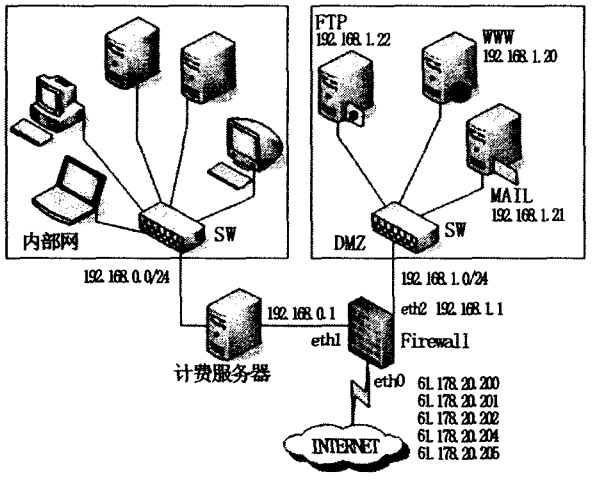

图 4 甘肃地震信息网的网络结构图

Fig. 4 Structure of Gansu Seismic Information Network.

3 甘肃地震信息网防火墙实例

3.1 网络结构

甘肃地震信息网的网络结构为星型以太网结构，通过一条带宽为 10M 的光纤连接到互联网，并对内、对外提供 WWW、E_MAIL 和 FTP 服务。甘肃地震信息网共有 16 个固定的因特网 IP 地址资源，其内部网络全部使用私有 IP 地址，通过 NAT 服务器带动局域网上网。为了更加有效地保证内部网络的安全，我们将对外服务的三台主机放到 DMZ 区(非军事区)，如图 4 所示。

由图 4 可以看出，作为防火墙的主机有 3 个网络接口，其中 eth0 连接外部网络，eth1 连接内部网，eth2 连接 DMZ 区。eth1 的 IP 地址是 192.168.0.1，它是内部网络 192.168.0.0/24 的出口网关；eth2 的 IP 地址为 192.168.1.1，它是 DMZ 区 192.168.1.0/24 的出口网关。我们在 eth0 上共配有 5 个 IP 地址，其中 61.178.20.204 和 61.178.20.205 是内部网络到互联网的出口。之所以用了两个 IP 地址，目的是为了起到负载均衡。61.178.20.200、61.178.20.201、61.178.20.202 分别是 WWW、FTP、E_MAIL 服务器的外网地址，通过 NAT 与 DMZ 区的三台服务器的内部地址建立一对一映射。

3.2 基本安全策略

(1)内网可以访问外网。内网的用户显然需要自由地访问外网。在这一策略中，防火墙需要进行源地址转换。

(2)内网可以访问 DMZ。此策略为了方便内网用户使用和管理 DMZ 中的服务器。

(3)外网不能访问内网。很显然，内网中存放的是企业内部数据，这些数据不允许外网的用户进行访问。

(4)外网可以访问 DMZ。DMZ 中的服务器本身就是要给外界提供服务的，所以外网必须可以访问 DMZ。外网访问 DMZ 需要由防火墙完成外网地址到服务器实际地址的转换。

(5)DMZ 不能访问内网。很明显，如果违背此策略，则当入侵者攻陷 DMZ 时，就可以进一步进攻到内网的重要数据。

(6)DMZ 不能访问外网。此条策略也有例外，比如对于 DMZ 中的邮件服务器，就需要访问外网，否则将不能正常工作。

另外，为了保证内部网络有足够的安全性，我们则采取了“没有明确允许的都被拒绝”的安全策略。即首先禁止所有入站信息包，然后再根据需要的服务允许特定的信息包通过防火墙。其初始化命令如下：iptables-P INPUT DROP，iptables-P OUTPUT DROP，iptables-P FORWARD DROP。

3.3 基本 filter 表的规则配置

(1) 处理“坏”TCP 包的链。首先，检查入站 TCP 包的包头，对不正常的包头数据，如：没有设置 SYN 但却是 NEW 状态的 TCP 包和那些设置了 SYN/ACK 位，但也被认为是 NEW 状态的 TCP 包，还有那些状态为 INVALID 的数据包都要被过滤掉，即 DROP 或 REJECT。下面的代码创建了一个用户自定义的名为 bad_tcp_packets 的处理“坏” TCP 包的链。

iptables_A bad_tcp_packets_p tcp_tcp_flags SYN, ACK SYN, ACK_m state－state NEW_j REJECT－reject_with tcp_reset

iptables_A bad_tcp_packets_p tcp ! －syn_m state－state NEW_j LOG－log_prefix "New not

syn:"

iptables_A bad_tcp_packets_p tcp ! —syn_m state—state NEW_j DROP

(2) 处理允许通过的 TPC 包。创建一个处理正常的 TCP 数据包的用户自定义链,名为 allowed,代码如下

iptables_A allowed_p TCP—syn_j ACCEPT

iptables_A allowed_p TCP_m state—state ESTABLISHED, RELATED_j ACCEPT

iptables_A allowed_p TCP_j DROP

(3) 处理 ICMP 包的链。对于入站的 ICMP 包,我们只接受三种类型的包:ICMP Echo requests,TTL equals 0 during transit 和 TTL equals 0 during reassembly。即允许类型为 8 和类型为 11 的 ICMP 包通过。其用户自定义链 icmp_packets 的代码如下:

iptables_A icmp_packets_p ICMP_i eth0_s 0/0_icmp_type 8_j ACCEPT

iptables_A icmp_packets_p ICMP_i eth0_s 0/0—icmp_type 11_j ACCEPT

(4) 处理 UDP 包。对于 UDP 包,由于它是一种无连接协议,所以在打开、关闭连接以及在发送数据时没有多少标记要设置,它也不需要任何类型的确认。但多数情况下,人们都习惯使用 ICQ、MSN、QQ 等多媒体在线聊天工具,所以应该对 UDP 的下列端口开放。其处理 UDP 包的用户自定义链 udp—packets 的代码如下:

iptables_A udp_packets_p UDP_s 0/0—destination_port 123_j ACCEPT

iptables_A udp_packets_p UDP_s 0/0—destination_port 2074_j ACCEPT

iptables_A udp_packets_p UDP_s 0/0—destination_port 4000_j ACCEPT

iptables_A udp_packets_p UDP_s 0/0—destination_port 8000_j ACCEPT

(5) 处理 TCP 包。通常,应该开放 21、22、23、25、80、110、113 端口,允许 ftp、telnet、ssh、smtp、http、pop3 服务。其代码如下:

iptables_A tcp_packets_p TCP_s 0/0_m multiport_destination_port 21,22,23,53,80,110,113_j allowed

3.4 DMZ 区的规则配置

(1) 外网可以访问 DMZ。为了保护 DMZ 中的服务器,外网对 DMZ 的访问也要加以限制。通常的思路是,只允许外网访问 DMZ 中服务器所提供的特定服务:

iptables_A FORWARD_i eth0_o eth2_m state—state ESTABLISHED,RELATED_j ACCEPT

允许外网访问 DMZ 中的 WWW 服务器:

iptables_A FORWARD_p TCP_i eth0_o eth2_d 192.168.1.20—dport 80—syn_j ACCEPT

iptables_A FORWARD_p ICMP_i eth0_o eth2_d 192.168.1.20_j icmp_packets

允许外网访问 DMZ 中的 FTP 服务器:

iptables_A FORWARD_p TCP_i eth0_o eth2_d 192.168.1.22—dport 21—syn_j ACCEPT

iptables_A FORWARD_p ICMP_i eth0_o eth2_d 192.168.1.22—j icmp_packets

允许外网访问 DMZ 中的 MAIL 服务器:

iptables_A FORWARD_p TCP_i eth0_o eth2_d 192.168.1.21—dport 25—syn_j ACCEPT

iptables_A FORWARD_p TCP_i eth0_o eth2_d 192.168.1.21—dport 80—syn_j ACCEPT

iptables_A FORWARD_p TCP_s 192.168.1.21_i eth2—dport 25_j ACCEPT

iptables_A FORWARD_p ICMP_i eth0_o eth2_d 192.168.1.21_j icmp_packets

(2) 外网不能访问内网。对应的防火墙脚本如下:

iptables_A FORWARD_i eth0_o eth1_j DROP

或

iptables_A FORWARD_i eth0_d 192.168.0.0/24_j DROP

以上命令将来自外网、去往内网的数据包全部丢弃。

(3) DMZ 不能访问内网。对应的防火墙脚本如下:

iptables_A FORWARD_i eth2_o eth1_m state—state ESTABLISHED,RELATED_j ACCEPT

iptables_A FORWARD_s 192.168.1.0/24_d 192.168.0.0/24_i eth2_j DROP

iptables_A FORWARD_i eth2_o eth1_j DROP

以上命令将丢弃所有从 DMZ 到内网的数据包。

(4) DMZ 可以访问外网。对应的防火墙脚本如下:

iptables_A FORWARD_i eth2_o eth0_j ACCEPT

(5) 内网可以访问 DMZ

iptables_A FORWARD_i eth1_o eth2_j ACCEPT 或

iptables_A FORWARD_i eth1_s 192.168.0.0/24_d 192.168.1.0/24_j ACCEPT

以上命令允许所有来自内网、目的地为 DMZ 的数据包通过。

3.5 NAT 表的规则配置

(1)带动局域网上网。局域网内的所有主机访问互联网是通过防火墙的 NAT 功能实现的。即对流出的数据包作 SNAT 操作,相应的防火墙脚本如下:

iptables_t nat_A POSTROUTING_s 192.168.0.0/24_o eth0_j SNAT—to 61.178.20.204—61.178.20.205 或

iptables_t nat_A POSTROUTING_o eth0_j SNAT—to_source 61.178.20.204—61.178.20.205

当数据包从连接外网的 eth0 流出时,防火墙将来自内网的数据包的源地址转换成外网的真实 IP 地址,也就是 61.178.20.204 或 61.178.20.205。这样,局域网中的主机就能和互联网上的主机进行通信,实现局域网上网。

(2)外网可以访问 DMZ 区的服务。外网要访问 DMZ 区中主机也是通过防火墙的 NAT 功能实现的,DMZ 区的主机对外提供各种服务,如 WWW、FTP、E_MAIL 等,且每台服务器都有一个真实的互联网 IP 地址与 DMZ 中的内部地址一一对应。所以要对进入防火墙的信息包所 DNAT 操作。其相应的脚本代码如下:

WWW 服务:iptables_t nat_A PREROUTING_p TCP_i eth0_d 61.178.20.200—dport 80_j DNAT—to_destination 192.168.1.20

FTP 服务:iptables_t nat_A PREROUTING_p TCP_i eth0_d 61.178.20.202—dport 21_j DNAT—to_destination 192.168.1.22

E_MAIL 服务: iptables_t nat_A PREROUTING_p TCP_i eth0_d 61.178.20.201_m multiport—destination_port 25,80,110_j DNAT—to_destination 192.168.1.21

iptables_t nat_A POSTROUTING_p tcp_s 192.168.0.21—dport 25_o eth0_j SNAT—to 61.178.20.201

4 部署和运行防火墙脚本

在 RedHat Linux 9.0 下部署 iptables 防火墙非常容易:只需将上述代码保存到/etc/rc.d/目录下文件名为 firewall(也可以是其它名称)的 shell 脚本文件中,修改 firewall 文件的属性,使其可执行,然后运行这个 shell 脚本即可。为了使 firewall 在系统启动时自动运行,可以编辑/etc/rc.d/rc.local 文件,在其中加上这样的命令行:"/etc/rc.d/firewall"。

当然,要使防火墙能够正常工作,我们还必须打开 Linux 系统内核的 IP 转发功能,即在 firewall 脚本文件的前面加上这样一行:"echo "1" >/proc/sys/net/ipv4/ip_forward";另外,还必须加载必需的 netfilter 内核模块,即在 firewall 脚本的前面应该加上下面这些代码:

```
/sbin/depmod_a
/sbin/modprobe ip_tables
/sbin/modprobe ip_conntrack
/sbin/modprobe iptable_filter
/sbin/modprobe iptable_mangle
/sbin/modprobe iptable_nat
/sbin/modprobe ip_nat_ftp
/sbin/modprobe ip_conntrack_ftp
/sbin/modprobe ipt_LOG
/sbin/modprobe ipt_limit
/sbin/modprobe ipt_state
```

5 测试

我们编写了一个脚本程序来对防火墙进行测试,测试 iptables 中的所有链及其规则。实际上,这个脚本就是使用了 iptables 的 LOG 功能,记录下了所有的 ping 请求和应答。通过这种方式,我们就可以了解哪些链被穿越了以及被穿越的顺序。使用方法如下,先执行这个脚本文件,再发布一个 ping 命令,如:ping_c 1 www.gssb.gov.cn,然后用命令 tail_n 0_f /var/log/messages 就可看到用了哪些链以及是什么顺序,除非记录因某些原因被替换了。

6 几点认识

(1) 包过滤防火墙是最常用的防火墙网关技术,是一种通用、廉价、有效的安全手段,性价比高。它只使用一个路由器就可以使企业的局域网连接到互联网上,而无需额外的费用,所提供的保护对于一般的小规模网络而言已经足够了,能很大程度地满

足单位的安全要求。

(2) 包过滤防火墙的优点是不用改动客户机和服务器上的应用程序,也不用改动原有的网络结构,对用户是透明的。它工作在网络层和传输层,处理IP包的速度比代理服务器快。但其弱点也是很明显的:因为过滤的只是网络层和传输层的有限信息,因而各种安全要求不可能充分满足,如不能提供有效的用户身份验证,缺少审计和报警机制,缺少上下文关联信息,不能有效地防范像病毒这类东西的入侵。另外,大多数过滤器中管理方式和用户界面较差;对安全管理人员素质要求高,建立安全规则时,必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此,在安全要求高的网络中过滤器通常是和应用网关(Application Gateway)配合使用,共同组成复合型防火墙系统。

(3) netfilter/iptables 是一个功能强大的基于状态的包过滤防火墙工具。iptablse 允许建立有状态的防火墙系统,可以有效地配置 WWW、FTP、E_MAIL 等网络服务,能够过滤 TCP 标志的任意组合报文,还能够过滤 MAC 地址,支持网络地址转换(NAT)和透明代理,而且系统日志配置容易,扩展性好。对于一个小型的不太复杂的网络,使用 netfilter/iptables 构建包过滤防火墙是一个理想的选择,价格便宜,只需一台运行 Linux 的普通计算机就可以了。

[参考文献]

[1] 梁如军,丛日权,等. Red Hat Linux 9 网络服务[M]. 北京:机械工业出版社,2003.

[2] Christopher Negus 著. 梁杰,巩樱,等译. Red Hat Linux 8 宝典[M]. 北京:电子工业出版社,2003.

[3] RFC1631. The IP Network Address Translator(NAT). 1994.

[4] RFC792. Internet Control Message Protocol. 1981.

[5] RFC793. Transmission Control Protocol. 1981.

[6] 游文南. 浅论网络防火墙技术[Eb/OL]. http://www.edu.cn/20020816/3064482.shtml.

[7] Rusty Russell. Linux 2.4 Packet Filtering HOWTO[Eb/OL]. http://linux.dalouis.com/doc/iptables/pfhtcn.html.

[8] Oskar Andreasson. Iptables Tutorial 1.1.19[Eb/OL]. http://www.jollycom.ca/iptables-tutorial/iptables-tutorial.html.