2001年 8月　　河 北 工 业 大 学 学 报　　August 2001
第30卷 第4期　　JOURNAL OF HEBEI UNIVERSITY OF TECHNOLOGY　　Vol.30 No.4

文章编号：1007-2373(2001)-04-0064-04

# Linux 防火墙规则的输入与验证

王永滨[1]，张 吉[2]

（1. 北京广播学院 计算机系，北京 100024；2. 河北工业大学 电气信息学院，天津 300130）

**摘要**：介绍了具有规则相容性形式化验证功能的 Linux 防火墙可视化输入系统，它增强了 Linux 防火墙的可操作性和规则完整性.

**关 键 词**：Linux；防火墙；验证；输入

**中图分类号**：TP311　　**文献标识码**：A

## 0 引言

Redhat Linux 6.2 系统中所带的防火墙 ipchains 具有强大的包过滤功能，但是 ipchains 的配置所要参数很多，相当繁琐. 鉴于此情况我们为 Linux 防火墙开发了可视化输入系统，通过此系统可以很方便的利用浏览器对防火墙进行配置，而不用再去记那些繁琐的 ipchains 命令. 系统根据输入的规则自动生成 ipchains 脚本，从而既减轻了管理人员的工作难度，又保留 ipchains 的强大功能.

虽然防火墙规则的可视化输入避免了规则的语法错误，但规则是上下文相关的，规则之间是否相容，是否有无用的规则，一般需由用户自己判断，当规则较多时，很容易出错. 这里我们提出了一种可机械执行的规则相容性形式化验证方法，辅助用户输入防火墙规则.

## 1 防火墙规则的可视化输入

利用 Web 浏览器进行防火墙规则的录入，界面如图 1. 其中：规则号表示这条规则放在过滤规则表中的位置，如不填写规则号，则默认是新增的一条规则，放在规则表的最后；源地址、目地地址表示包过滤所要检查的网络 IP 地址；协议为选择该条规则所用的协议，在防火墙规则中一般常用的协议为 TCP，UDP，ICMP；服务指所要禁止的或要放行的服务，即相当于 TCP、UDP 协议所用的端口号；动作即 ipchains 的 action，在本系统中只是采用了 DENY，ACCEPT，FORWARD；日志表示选择是否要日志，记录一下包过滤的情况；方向为进入、输出.


图 1 录入界面

输入的防火墙保存在 rulesets 文件中，如图 1 中所显示的内容会在 rulesets 文件中增加如表 1 所示的一行：

收稿日期：2001-05-16
作者简介：王永滨（1964-），男（汉族），教授.

表 1 图 1 中所示内容在 rulesets 文件中增加的一行

| 源地址 | 目标地址 | 协议 | 服务 | 动作 | 日志 | 方向 |
|---|---|---|---|---|---|---|
| Abc | inter | Tcp | www | ACCEPT | YES | IN |

生成防火墙脚本函数 gen_script () 会将此条翻译为如下一条 ipchains 规则：

/sbin/ipchains -A input -p tcp -s $abc -d $inter --dport www -j ACCEPT -l

其中 abc 和 inter 为 IP 地址，如：

abc='192.168.1.82/24'

inter='192.168.1.1/24'

## 2 规则相容性验证

检查进入过滤规则表 rulesets 文件中的所有规则的相容性，如果新输入的某条规则与现有规则表中的其他规则不相容或为规则表中所有规则的逻辑结论，则这条规则不能进入过滤规则表中，需提醒用户．即：

如果新加入的规则与前面所有规则的合取式是永假的，则与前面的规则不相容，此时该规则不应加入规则表中，如果新加入的规则是前面规则的逻辑结论，则这是一条多余的规则．也不应加入规则表中．

对于新输入的规则是否为前面所有规则的逻辑结论，其证明可归结为不相容性的证明．

引理：G 为 F1，F2,.....，Fn 的逻辑结论，当且仅当（F1∧F2∧..... ∧Fn）⇒G

定理：G 为 F1，F2,.....，Fn 的逻辑结论，当且仅当（F1∧F2∧..... ∧Fn）∧～G 是不相容的．

对于不相容性的验证使用鲁宾逊消解原理，以便于计算机自动完成．

首先将欲证为不可满足的谓词公式变化为斯柯林标准形，然后变为子句集并用鲁宾逊消解原理证明其不可满足性．

例如：表 2 所示的两条防火墙规则显然第二条是多余的，即它为上面规则的逻辑结论．

表 2 两条防火墙规则

| 规则号 | 方向 | 动作 | 源地址 | 目标地址 | 服务 |
|---|---|---|---|---|---|
| 1 | 进 | 通过 | all | Addr1 | all |
| 2 | 进 | 通过 | all | Addr1 | 80 |

证明：设

RA (x)：目标地址是 x；LA (x)：源地址是 x；RP (x)：服务是 x；P：通过．则：

～RA (x)：目标地址不是 x；～LA (x)：源地址不是 x；～RP (x)：服务不是 x；～P：阻止．

1）规则可写成如下形式

$$\forall y \forall z(RA(addr1) \wedge RP(y) \wedge LA(z) \rightarrow P) \quad (1)$$

$$\forall z(RA(addr1) \wedge RP(80) \wedge LA(z) \rightarrow P) \quad (2)$$

欲证 (2) 是 (1) 是逻加结论只须证～ (2) 与 (1) 是不可满足的；

2）变成斯柯林标准型

$$(1) \Leftrightarrow \forall y \forall z(\sim RA(addr1) \vee \sim RP(y) \vee \sim LA(z) \vee P)$$

省去全称量词

$$\sim RA(addr1) \vee \sim RP(y) \vee \sim LA(z) \vee P$$

$$\sim(2) \Leftrightarrow \sim(\forall z(\sim(RA(addr1) \wedge RP(80) \wedge LA(z)) \vee P)) \Leftrightarrow (z\ (RA(addr1) \wedge RP(80) \wedge LA(z) \wedge \sim P)$$

去掉存在量词

$$RA(addr1) \wedge RP(80) \wedge LA(z) \wedge \sim P$$

3) 消解

| | | |
|---|---|---|
| ～RA(addr1)∨～RP(y)∨～LA(z)∨P | (3) | |
| RA (addr1) | (4) | |
| RP(80) | (5) | |
| LA (c) | (6) | |
| ～P | (7) | |
| ～RP (y) ∨～LA (z) ∨P | (8) | ((3), (4)) |
| ～LA (z) ∨P | (9) | ((8), (5) δ= {80/y}) |
| P | (10) | ((9), (6) δ= {c/z}) |
| □ | | ((10), (7)) |

由上面的证明可知防火墙第二条规则是第一条规则的逻辑结论．第二条规则是重复的．不应存入防火墙规则表中．

## 3 各链之间的规则检查

当用户在某条链中输入一条规则后，有可能出现与其它链中的规则相冲突的现象，本系统能自动根据情况进行判断，给出用户提示，做出相应调整．

### 3.1 规则的冲突情况分类

3.1.1 同时出现的规则

有一些规则，当某链中该条规则出现时，一定要在其他链中有一条相对应的规则．如：

1）如果在转发链中有一条对来自某一地址的包转发的规则，则进入链必须允许该地址的包进入，同时输出链必须允许该地址的包出去．

2）如 output 链中有对某一地址的包允许通过的规则，则 input 链必须允许此地址的包进入．

3.1.2 冲突的规则

当在某条链中输入一条规则时，有可能出现与其它的链中的某条规则，或规则的组合结果发生冲突的情况，这时应提示用户冲突情况，显示冲突的规则，让管理人员进行调整．

如在进入链中对来自某地址的包 DENY 或 REJECT 后，又在转发链中存在一条规则对该地址的包进行了转发．此时应向用户提示．

### 3.2 实现方法

将有可能发生冲突的规则存入文件 CheckRule 中，相当于过滤规则库，用户可以根据自己的经验，按一定的格式增加或修改过滤规则．这样可以使系统的检测功能越来越强，及时调整．文件的结构分为两部分，一部分是“必须存在的规则"，另一部分是“相冲突的规则”．每条过滤规则分为两段，前面一段为输入规则形式，后面一段为相对应的要求存在的或相冲突的规则．

内容如下：

```
## The rules that must be exist together!
## 格式：源 目标 协议 端口 动作 日志 方向
## 前面是新加的规则，后面是必须存在的
    Sour Dest tcp Port ACCEPT Log forward
                | Sour ALL tcp Port ACCEPT Log input
#对某个数据包要转发时，在 input 链中一定要有一条允许与此包的源地址、端口、协议相同
```

的包通过的规则

Sour Dest tcp Port ACCEPT Log forward

| ALL Dest tcp Port ACCEPT Log output

#对某个数据包转发时，在 output 链中一定要有一条允许与此包目标地址、协议相同的包通过的规则

.....

## The rules that conflict with each other!

## 格式：源 目标 协议 端口 动作 日志 方向

## 前面是所输入的规则，后面是相冲突的规则

Sour Dest tcp Port ACCEPT log forward

| Sour ALL tcp Port DENY log input

#当对某个包要转发时，在 input 链中存在一条允许与此包源地址、协议相同的包被禁止的规则

Sour Dest tcp Port ACCEPT log forward

| ALL Dest tcp Port DENY log output

#当对某个包要转发时，在 output 链中存在一条允许与此包目标地址、协议相同的包被禁止的规则

.....

程序流程如图 2.

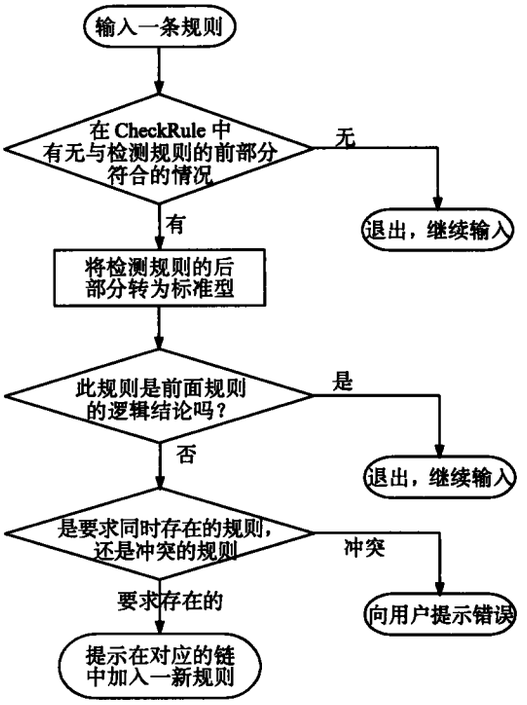


图 2 程序流程图

## 4 结束语

Linux 防火墙是开放的、免费的，并具有强大的包过滤功能，加入具有规则自动验证功能的可视化输入系统，使用更加方便，应用将更广泛.

## 参考文献：

[1] Paul Russell. Ipchains-HOWTO [EB/OL]. http: //www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.

[2] 赖阿福，商健智. Linux 技术参考手册网络篇 [M]. 北京：中国铁道出版社，2000.

[3] 尼尔逊 N J. 人工智能原理 [M]. 北京：科学出版社，1983.

# Visual Input and Verification of Linux Firewall Rule

WANG Yong-bin[1]，ZHANG Ji[2]

( 1. Computer Department, Beijing Broadcasting Institute, Beijing 100024, China; 2. School of Electrical Engineering and Information Technology, Hebei University of Technology, Tianjin 300130, China )

**Abstract**: A visual input system of Linux Firewall is introduced, which has the function of the rules compatible formalized verification. It makes the operation of Linux Firewall simplified and the rule integrality improved.

**Key words**: Linux; firewall; verification; input