文章编号：1006-4354（2006）04-0045-02

路由器访问列表与网络安全

王 云，刘晓利，马 峰
（榆林市气象局，陕西榆林 719000）

中图分类号：P409 文献标识码：B

访问列表是网络管理员在路由器中加入控制数据包输入、输出的规则，不是由路由器自己产生的。访问列表能够允许或禁止数据包进入或输出到目的地，当数据包经过路由器某一个端口转发时，必须先在访问列表里查找匹配条件，如果允许，则通过。使用访问列表步骤：一是通过指定访问列表名称及访问条件，建立访问列表；二是将访问列表应用到接口。本文以市级气象局使用的BDCOM2621路由器为例，探讨路由器访问列表与网络安全。

1 建立访问列表

BDCOM2621路由器访问列表分为标准访问列表和扩展访问列表。标准访问列表通过使用IP包中的源IP地址过滤网络流量。扩展访问列表允许指定源地址和目的地址，及表示上层协议或应用的协议和端口号，通过使用扩展的访问列表，可以有效地允许用户访问物理LAN的同时禁止访问特定的主机及主机的特定服务。

1.1 建立标准访问列表

建立标准访问列表，需进入BDCOM2621路由器全局配置态，执行命令：

ip access－list standard name//使用名字定义一个标准访问列表。

{deny | permit}{source [source－mask] | any} [log] //在标准访问列表配置模式下，指定一个或多个允许或禁止条件。Source表示源网络地址或主机号，用32位二进制表示，使用关键字Any作为0.0.0.0 0.0.0.0的源地址和源掩码的缩写；Log表示可以进行日志记录。

Exit//退出访问列表配置模式。

1.2 建立扩展访问列表

建立扩展访问列表，需进入BDCOM2621路由器全局配置态，执行命令：

ip access－list extended name//使用名字定义一个扩展访问列表。

{deny | permit} protocol source source－mask [operator port] destination destination－mask [operator port] [icmp－type] [igmp－type] [precedence precedence] [tos tos] [established] [log] //在扩展访问列表配置模式下，指定一个或多个允许或禁止条件。protocol表示协议名称或协议号，可以是关键字IGMP、ICMP、TCP、UDP、OSPF、IP、IGRP等，也可以是表示IP协议号0～255的任何一个整数；Operator表示比较源或目标端口，包括Lt（小于）、Gt（大于）、Eq（等于）和Neq（不等于）；Icmp－type表示Icmp包可由Icmp报文类型过滤，类型是数字0～255；Igmp－type表示Igmp包可由Igmp报文类型过滤，类型是数字0～15；Precedence表示数据包可以由优先级过滤，用数字0～7指定；Tos表示数据包可以使用服务层过滤，用数字0～15指定；Establishd只适用于TCP协议，表示一个已建立的连接。Exit//退出访问列表配置模式。

2 将访问列表应用到接口

建立了访问列表后，可以将它应用到一个或

收稿日期：2006-03-17

作者简介：王云（1978-），男，陕西子洲人，学士，从事网络管理维护工作。

多个接口上，分为进或出两种情况。进入BDCOM2621路由器接口配置态，使用命令：ip access－group name {in | out} //将访问列表应用到接口。In 表示进接口时使用访问列表，Out 表示出接口时使用访问列表。

访问列表可用在出接口也可用在入接口。标准的入口访问列表，接收到数据包后，对照访问列表检查包的源地址。对扩展的入口访问列表，路由器也检查目标地址。如果访问列表允许该地址，则继续处理该数据包。如果访问列表禁止该地址，放弃数据包并返回一个 ICMP 主机不可到达报文。标准的出口访问表，接收和路由一个数据包到控制接口后，对照访问列表检查数据包的源地址。对于扩展的出口访问列表，路由器还检查接收端的访问列表。如果访问列表允许，就传送数据包。如果访问列表禁止该地址，则放弃数据包并返回一个 ICMP 主机不可达报文。

3 应用举例

3.1 封掉常见的病毒攻击端口

135、137、139 和 445 等端口是 Windows 系统默认开放的端口，对这些端口的访问应该加以限制，否则系统就很容易受到攻击。

```
ip access-list extended rule1
deny   tcp any any eq 135
deny   tcp any any eq 139
deny   tcp any any eq 445
deny   tcp any any eq 593
deny   tcp any any eq 3333
deny   udp any any eq 135
deny   udp any any eq 137
deny   udp any any eq 138
deny   udp any any eq 4444
deny   udp any any eq tftp
```

rule1 可以应用在连接局域网接口的 In 方向。

3.2 防止外部的非法探测

非法访问者对内部网络发起攻击前，往往会用 ping 或其他命令探测网络，可以通过禁止从外部用 ping、traceroute 等探测网络来进行防范。

```
ip access-list extended rule2
deny icmp any any echo//阻止用 ping 探测网络
deny icmp any any time-exceeded//阻止用 traceroute 探测网络
permit ip any any
```

在外部接口的 Out 方向使用 rule2 过滤，主要是阻止答复输出，不阻止探测进入。

3.3 防止外部地址欺骗

外部网络用户可能会使用内部网合法 IP 地址或者回环地址作为源地址，实现非法访问。

```
ip access-list extended rule3
permit ip 172.23.64.0 255.255.255.0 any//允许省局访问
deny ip 172.23.0.0 255.255.0.0 any//阻止源地址为其它地市所有通信流
deny ip 127.0.0.0 0.255.0.0 .0 any//阻止源地址为回环地址的所有通信流
deny ip 224.0.0.0 255.0.0.0 any//阻止源地址为多目的地址的所有通信流
deny ip host 0.0.0.0 any//阻止没有列出源地址的通信流
```

外部接口的 In 方向使用 rule3。

4 注意

标准的访问列表和扩展的访问列表不能使用相同的名称。

访问列表中第一个匹配决定是否接受或拒绝该地址。因为在第一个匹配之后，就停止了匹配规则，所以条件的先后次序是重要的。

当建立访问列表时，缺省时访问列表的结尾包含隐含的 deny 语句。意味着如果数据包与访问列表中的所有行都不匹配，将被丢弃。

在初始建立访问列表后，任何后续的增加部分都放入表的尾部。