路由器访问控制列表在网络安全中的应用

潘文婵,章 韵
(南京邮电大学 计算机学院,江苏 南京 210046)

摘 要:访问控制列表(ACL)是解决和提高网络安全性的方法之一,是用来过滤与控制进出路由器数据流的一种访问控制技术,可以限制网络流量,提高网络性能,控制通信流量。文中探讨了访问控制列表的基本概念及工作原理,并列举了访问控制列表在网络安全方面的具体应用。结合配置实例,介绍如何在路由器下通过访问控制列表来构建计算机网络的防火墙体系结构,对局域网安全性能进行保护。在路由器下配置ACL,成为构建网络安全体系的一种技术手段。

关键词:访问控制列表;路由器;网络安全
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2010)08-0159-04

Application of Access Control List on Router in Network Security

PAN Wen-chan, ZHANG Yun
(College of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210046, China)

Abstract: Access control list (ACL) is proposed to solve or improve the network security problem. ACL is an access and control technology which is used to filter and control the data flow in the routers. ACL can improve the network performance and control the flow of traffic. The basic conception and the elements of the access control list are discussed. The application of ACL in the network security is as listed. By giving several practical disposal examples, access control techniques on routers are used to analyze how to improve the network security performance to ensure the safety of network. Filtrating the information of network by ACL under the router becomes a technology means of structuring network security system.

Key words: access control list; router; network security

0 引 言

网络安全一直是倍受关注的领域,如果缺乏一定的安全保障,无论是公共网还是企业专用网都难以抵挡网络攻击和非法入侵。随着人们对网络依赖程度的日益增强,网络的安全性和可靠性问题愈来愈重要,一旦网络瘫痪或重要信息被窃取,将带来巨大损失。而路由器作为网络传输过程中的重要设备,对报文安全、正确和快速的转发起着关键作用。路由器工作于网络层,是信息出入的必经之路,为通过路由器的数据帧选择最佳传输路径,并将之传送到目的站点[1]。路由器能降低系统负荷,限制流量,节约资源,保护局域网的安全,防止外网用户非法探测。因而路由过滤对网络的安全具有举足轻重的作用。在路由器上配置访问控制列表(Access Control List),通过访问规则,控制和过滤经过路由器的数据流[2],隔离外网和内网,防止外部用户对内部网络不安全的访问,是实现基本的网络安全手段之一。

收稿日期:2010-01-25;**修回日期**:2010-04-17
基金项目:南京邮电大学教学改革研究项目(JG00406JX15)
作者简介:潘文婵(1983-),女,江苏南京人,硕士,助教,研究方向为计算机网络通信;章 韵,硕士,副教授,研究方向为计算机技术在通信中的应用。

1 访问控制列表

1.1 访问控制列表的概念

访问控制列表简称ACL,使用包过滤技术,告诉路由器接受哪些数据包、拒绝哪些数据包。访问控制列表由源地址、目的地址、端口号等一系列特定指示条件组成,将数据包中的信息与访问控制列表参数匹配从而过滤进出路由器接口的数据包,保护路由器和网络的安全[3]。

1.2 访问控制列表功能

以下为访问控制列表的功能:

(1)控制系统的网络流量,改善网络性能。

(2)控制系统的通信流量。

(3)保障网络的安全访问[4]。例如,访问控制列表允许主机A访问指定网络,而拒绝主机B访问。

(4)在路由器接口处,决定哪种类型的通信流量被

转发,哪种类型的通信流量被拒绝。

1.3 访问控制列表分类

访问控制列表分为标准访问控制列表和扩展访问控制列表两种。

(1)标准访问控制列表:如果允许某一网络的所有通信流量通过,或者拒绝某一特定网络的所有通信流量,可以使用标准访问控制列表。标准访问控制列表通过对 IP 包中的源地址或源地址中的一部分进行过滤,可对匹配的包采取拒绝或允许两个操作。

标准访问控制列表的语法格式:

access - list access - list - number[permit/deny] source - address[wildcard mask]

其中 access - list - number 表示标准访问控制列表的号码,编号范围是从 1 到 99;permit/deny 表示该访问控制列表是允许还是拒绝数据包;source - address 表示主机或网络的源地址;wildcard mask 表示通配符掩码,在访问列表中将通配符掩码中的一位设成 1 表示 IP 地址中对应的位既可以是 1 又可以是 0,此位又称为"无关"位。掩码位设成 0 则表示 IP 地址中相对应的位必须精确匹配[5]。

(2)扩展访问控制列表:扩展访问控制列表比标准 IP 访问控制列表具有更多的匹配项,可以针对包括源地址、源端口、目的地址、目的端口、协议类型和 TCP 连接建立等进行过滤。扩展访问控制列表比标准访问控制列表更具有灵活性和可扩充性。使用扩展访问控制列表,通常允许、拒绝的是某个特定的协议。

一个扩展的 ACL 的一般语法格式:

access - list[list number][permit/deny][protocol][source address][source - wildcard][source port][destination address][destination - wildcard][destination port][log][option]

其中 list number 表示扩展访问控制列表的号码,编号范围是从 100 到 199。permit/deny 表示该访问控制列表是允许还是拒绝数据包。protocol 表示协议项,指出哪些协议需要被过滤,例如 TCP、IP、UDP、ICMP 等。source address、source wildcard 表示源地址和通配符屏蔽码。source port 表示源端口号,源端口号可以使用一个数字或者使用一个可识别的助记符。例如,可以使用 80 或者 http 来指定 Web 的超文本传输协议。对于 TCP 和 UDP,可以设置和使用操作符"<"(小于)、">"(大于)、"="(等于)以及"≠"(不等于)。destination address、destination wildcard 表示目的地址和通配符屏蔽码。destination port 表示目的端口号,可以使用数字、助记符或者使用操作符与数字或助记符相结合的格式来指定一个端口范围。log 表示日志记录,对那些能够匹配访问表中的 permit 和 deny 语句的报文进行日志记录。日志信息包含访问表号、报文的允许或拒绝、源 IP 地址以及在显示了第一个匹配以来每 5 分钟间隔内的报文数目。

1.4 访问控制列表的工作流程

当路由器的接口接收到一个数据包时,首先会检查访问控制列表,访问控制列表对符合匹配规则的数据包进行允许和拒绝的操作,被拒绝的数据包将会被丢弃,允许的数据包进入路由选择状态。

对进入路由选择状态的数据再根据路由器的路由表执行路由选择,如果路由表中没有到达目标网络的路由,那么相应的数据包就会被丢弃;如果路由表中存在到达目标网络的路由,则数据包被送到相应的网络接口。

访问控制列表其实就是各种允许或者拒绝的条件判断语句的集合,其特点是根据从上到下的语序进行判断,当第一个条件满足时,就不会再对其他条件进行比较,因此在访问控制列表中各条件语句的放置顺序非常重要,不注意这一点往往会使得访问控制列表形同虚设[6]。CISCO 路由器中,访问控制列表的最后一句是隐含的拒绝所有(deny any any),表示不匹配访问控制列表语句的报文要被丢弃掉[7]。

1.5 访问控制列表的配置

在一个接口上配置访问控制列表,步骤如下:

(1)定义访问控制列表。

(2)指定访问控制列表所作用的接口。

(3)定义访问控制列表作用于接口上的方向。

访问控制列表规则定义后,必须应用到路由器的某个接口上,并指明在接口上是 out 还是 in 方向。注意接口方向是以路由器为参考点,即进入路由器为 in 方向,出路由器为 out 方向。定义 ACL 所应用的接口方向,通常使用 ip access - group 命令来指定。方向用于指出,在数据包进入或离开路由器接口时对其进行过滤。

在同一端口上应用访问控制列表的 in 语句或 out 语句只能有一条,如需将两组访问列表应用到同一端口上的同一方向,需将两组访问控制列表进行合并处理,才能应用。

2 访问控制列表在网络安全中的应用

2.1 防止病毒传播和黑客攻击

针对微软操作系统的漏洞,一些病毒程序和漏洞扫描软件通过 UDP 端口 135、137、138、1434 和 TCP 端口 135、137、139、445、4444、5554、9995、9996 等进行病毒传播和攻击[8],可如下设置访问控制列表阻止病

毒传播和黑客攻击。

access－list 101 deny udp any any eq 135
access－list 101 deny udp any any eq 137
access－list 101 deny udp any any eq 138
access－list 101 deny udp any any eq 445
access－list 101 deny udp any any eq 1434
access－list 101 deny tcp any any eq 135
access－list 101 deny tcp any any eq 137
access－list 101 deny tcp any any eq 139
access－list 101 deny tcp any any eq 445
access－list 101 deny tcp any any eq 4444
access－list 101 deny tcp any any eq 5554
access－list 101 deny tcp any any eq 9995
access－list 101 deny tcp any any eq 9996
access－list 101 permit ip any any

最后一条语句很重要,允许其它所有数据包通过,如果没有,那么所有数据包都被拒绝进入内网,同样内网也无法访问外网。

2.2　防止外部非法探测和 IP 地址欺骗

如图 1 所示,交换机和路由器的 E1 端口相连,内部局域网通过路由器的 S0 接口和互联网连接。IP 欺骗指创建看起来似乎来自其他 IP 地址的数据包。黑客常采用一种称为 IP 地址欺骗的技术,他伪装成一个内部或可信任的外部 IP 地址来对目标进行攻击[9]。IP 欺骗攻击很难被检测,且需要技巧和方法来监控并分析数据包。可以在路由器的 S0 接口的入方向上建立访问控制列表进行阻止,防止外网的黑客通过扫描工具探测内网。

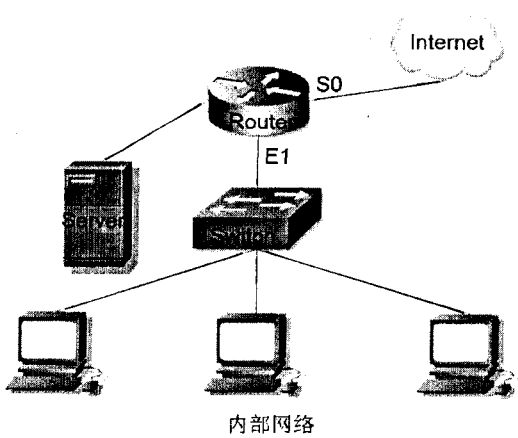

图 1　网络拓扑图

攻击者对内部网络进行非法访问前,通常会用 traceroute、ping 等命令嗅探网络,可以禁止从外部用 traceroute、ping 等这些命令来探测网络[10]。针对此问题,可建立如下访问控制列表:

access－list 102 deny icmp any any echo
access－list 102 deny icmp any any echo－reply
access－list 102 deny icmp any any unreachable
access－list 102 deny icmp any any traceroute

网络中存在一个安全隐患,那就是现在许多网卡都支持 MAC 地址重新配置,非法用户可以通过将自己所用网络设备的 MAC 地址改为合法用户 MAC 地址的方法,使用 MAC 地址“欺骗”,成功通过交换机的检查,进而入侵内部网络资源,造成不安全的隐患。对于此类问题,设置如下访问控制列表:

access－list 103 deny ip 10.0.0.0 0.255.255.255 any
access－list 103 deny ip 192.168.0.0 0.0.255.255 any
access－list 103 deny ip 172.16.0.0 0.0.255.255 any
access－list 103 deny ip 127.0.0.0 0.255.255.255 any
access－list 103 deny ip 224.0.0.0 0.255.255.255 any
access－list 103 deny ip host 0.0.0.0 any

2.3　上网时间控制

基于时间的访问控制列表是在扩展访问列表的基础上增加有效的时间范围来更灵活地配置网络。它首先定义时间段及时间范围,然后在扩展访问控制列表的基础上应用,适合于时间段的管理。

要想使基于时间的访问控制列表生效需要配置两方面的命令,首先定义时间段及时间范围,然后根据访问控制列表自身的配置,将详细的规则添加到访问控制列表中。基于时间的访问列表的设计中,time－range 命令用来定义时间范围,absolute 该命令用来指定绝对时间范围,periodic 主要是以星期为参数来定义时间范围的一个命令。一个时间范围只能有一个 absolute 语句,但是可以有几个 periodic 语句。命令格式为:

time－range time－range－name absolute[start time date][end time date]periodic days－of－the week hh:mm to[days－of－the week]hh:mm

基于时间的访问控制列表,可以根据用户要求的时间,比如一天中具体时间段或一周中的不同日期,过滤转发数据包。例如在学校,为了让学生安心学习,平时上课时间不允许学生上外网。这种情况仅仅通过发布通知规定是不能彻底杜绝学生逃课上网的问题,这时基于时间的访问控制列表应运而生。可以设置周一至周五上课时间(8:00～18:00)禁止访问外网,周末和晚上正常开放,配置如下:

Router(config)＃time－range schooltime
Router(config－time－range)＃absolute start 00:00 1 March 2010 end 23:59 14 July 2010
Router(config－time－range)＃periodic weekdays 8:00 to 18:00

Router(config)# access-list 104 deny ip any any time-range schooltime

Router(config)# access-list 104 permit ip any any

Router(config)# interface s0/0

Router(config-if)# ip access-list 104 out

以上定义了一个时间段,名称为 schooltime,并且设置了这个时间段的起始时间为 2010 年 3 月 1 日,结束时间为 2010 年 7 月 14 日,其中周一到周五,从早上 8 点到晚上 18 点不能访问外网。通过这个时间段和扩展访问控制列表的规则结合就可以制定出针对学校时间段开放的基于时间的访问控制列表了[11]。合理有效地利用基于时间的访问控制列表,可以更有效、更安全、更方便地保护内部网络。

2.4 对虚拟终端的访问控制

网络设备的安全对整个网络的安全非常重要,要确保设备安全,以避免受到攻击而造成不必要的损失。网络设备的访问控制主要目的是防止非法用户进入网络设备并对其配置进行非法修改,避免网络瘫痪[12]。虚拟端口相对于实端口而言,一般根据需要在路由器上虚拟出一些端口,这些端口被称为虚拟终端或虚拟端口。配置 vty 线路以便实现 Telnet 访问。虚拟终端线路用于实现对路由器的远程访问。默认情况下,路由器有 5 条终端线路(vty0-4),最多可以设置 16 条线路。在虚拟终端线路上实施访问控制列表,可以允许或拒绝用户通过虚拟端口访问路由器。简言之,仅允许某些 IP 地址或某些网络地址能够远程登录到路由器,保障网络安全。

例如只有 IP 地址为 192.168.10.10 的计算机可以 Telnet 到指定路由器。设置如下访问控制列表:

Router(config)# access-list 1 permit host 192.168.10.10

Router(config)# access-list 1 deny any

Router(config)# line vty 0 4

Router(config-line)# login

Router(config-line)# password 12345

Router(config-line)# access-class 1 in

3 访问控制列表应用实例

图 2 是访问控制列表应用拓扑图。现要求 PC1 所在网段只能访问服务器上的 WWW,而不能访问 FTP。

Router1(config)# access-list 105 permit tcp 172.16.1.0 0.0.0.255 host 172.16.3.2 eq www

Router1(config)# access-list 105 deny tcp 172.16.1.0 0.0.0.255 host 172.16.3.3 eq 21

Router1(config)# access-list 105 deny tcp 172.16.1.0 0.0.0.255 host 172.16.3.3 eq 20

Router1(config)# access-list 105 permit ip any any

由于 FTP 使用两个端口,其中 21 是控制通道,20 是数据通道,出于安全考虑,建议同时关闭 21 和 20 两个端口。还需要注意的是,在控制列表的最后一定要加上 access-list 105 permit ip any any 一句,否则其他网段的 PC 就无法访问 172.16.3.3 主机了,其原因是系统默认会在控制列表的最后加上 deny any any。

将访问控制列表应用到端口上。

Router1(config)# interface fa0/0

Router1(config-if)# ip access-group 105 in

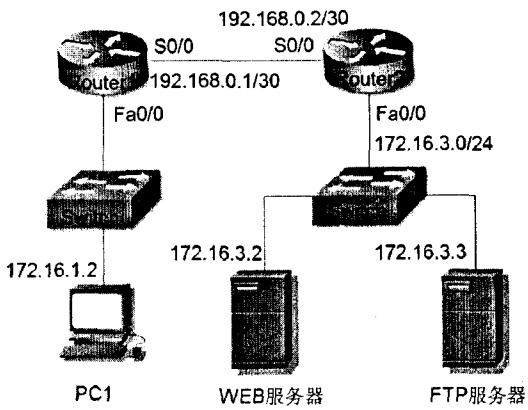

图 2 访问控制列表的应用拓扑图

4 结束语

介绍了访问控制列表(ACL)的基本概念、工作原理,及其在网络安全中的具体应用。访问控制是网络安全防范和保护的主要策略,它的主要任务是保证网络资源不被非法使用和访问。在路由器的接口上合理适当地配置访问控制列表后,可以对入站接口、出站接口及通过路由器中继的数据包进行安全检测,保障网络安全。

ACL 实现访问控制形式灵活、用途广泛,但也有其局限性。ACL 使用包过滤技术,过滤的仅仅只是第三层和第四层包头中的部分信息,因而无法识别到具体的人,无法识别到应用内部的权限级别等。因此,要达到端到端的权限控制目的,需要和系统级及应用级的访问权限控制结合使用。

参考文献:

[1] 黎连业,张 维,向东明.路由器及其应用技术[M].北京:清华大学出版社,2004.

[2] Malik.网络安全原理与实践[M].王宝生,朱培栋,白建军,译.北京:人民邮电出版社,2008.

(下转第 166 页)

表 4 网络系统安全态势指数值

时间	t_1	t_2	t_3	t_4
安全态势指数值	0.1932	0.2143	0.4234	0.0758
时间	t_5	t_6	t_7	t_8
安全态势指数值	0.7633	0.8724	0.8253	0.5651

通过表 4 的数据分析可以看出，该网络在时间段 t_1、t_2、t_4 内的安全态势指数值比较小，表明此阶段网络的状况比较安全、稳定；在时间段 t_3、t_5、t_8 内虽然遭受到一定的威胁，但还可以维持其运行状态。在 t_6，t_7 时刻，网络安全态势指数值很高，表明此时间段内网络遭受到较大的威胁，应该引起网络管理员的重视，采取必要的措施。

对照表 2，可以看出用文中设计的基于灰色理论的层次化网络安全态势评估方法得出的评估结果比较符合客观情况。

需要指出的是，以上的分析中，默认安全态势指数值与网络安全状态的对应关系为：

FL 在[0,0.3]之间，网络是安全的；

FL 在[0.31,0.8]之间，网络可正常运行；

FL 在[0.81,1]之间，网络遭受到的威胁严重，网络处于不安全的状态。

在实际运用中，管理人员可以根据安全防范需求，动态设置安全态势指数的阈值[12]。

4 结束语

文中设计了一种基于灰色理论的层次化网络安全态势评估方法，给出了层次化网络安全态势评估模型和安全态势指数的定量计算方法，并采用 Honeynet 数据集，利用所设计的方法，对网络中发生的网络安全事件和基于这些事件的网络安全态势评估过程进行了仿真和分析，给出了整个网络系统在实验所处环境下的安全状况。通过实验可以看出，文中设计的这种方法能比较有效而准确地评估网络的安全态势，这有助于网络管理员及时根据反馈信息进行安全措施调整，从而提高网络安全管理效率。

参考文献：

[1] 陈秀真，郑庆宏，管晓宏，等. 网络化系统安全态势评估的研究[J]. 西安交通大学学报，2004，38(4)：503－507.

[2] 王廷博，徐世超. 基于层次分析法的网络安全态势评估方法研究[J]. 电脑知识与技术，2008，5(4)：56－58.

[3] 刘思峰，党耀国，张岐山. 灰色系统理论及其应用[M]. 第 3 版. 北京：科学出版社，2004.

[4] 肖新平，宋中民，李 峰. 灰技术基础及其应用[M]. 北京：科学出版社，2005.

[5] 熊和金，陈绵云. 灰色关联度度公式的几种拓广[J]. 系统工程与电子技术，2000，22(11)：8－11.

[6] 唐志刚，赵建国，张 超. 灰色关联度分析法评判目标威胁度[J]. 火力与指挥控制，2004，29(6)：79－80.

[7] 朱振国，鄢 羽，张 闽，等. 一种量化的网络安全态势评估方法[J]. 微计算机信息，2007，23(3)：62－65.

[8] Feng D G，Zhang Y，Zhang Y Q. Survey of information security risk assessment[J]. Journal of China Institute of Communications，2004，25(7)：10－18.

[9] Martin R，Chris G. Snort users manual，Snort release2. 0. 0 [EB/OL]. 2002－07－06. http://www. snort. org/docs/SnortUsersManual. pdf.

[10] Honeynet Project. Know your enemy：statistics[EB/OL]. 2001－07－22. http://www. HoneyNet. org/papers/stats/.

[11] Honeynet Project. Scan 17[EB/OL]. 2002. http://www. honeynet. org/scans/scan17.

[12] 柯敏毅，肖俊林. 网络安全评估的量化研究[J]. 网络安全技术与应用，2006(9)：18－21.

(上接第 162 页)

[3] 范 萍，李罕伟. 基于 ACL 的网络层访问权限控制技术研究[J]. 华东交通大学学报，2004(4)：89－92.

[4] 洪新建，洪新华，谢庆华. 反射访问控制列表在网络安全中的应用[J]. 计算机安全，2007(3)：40－41.

[5] 曾旷怡，杨家海. 访问控制列表的优化问题[J]. 软件学报，2007，18(4)：978－986.

[6] Lammle T. CCNA 学习指南[M]. 北京：电子工业出版社，2004.

[7] Vatsavai R R，Chakravarthy S，Mohania M. Access Control Inference and Feedback for Policy Managers：A Fine－Grained Analysis[C]//IEEE International Workshop on Policies for Distributed Systems and Networks. London：[s. n.]，2006.

[8] 刘 军，王彩萍. ACL 在 IP 网络中的应用[J]. 计算机与数字工程，2009，37(1)：178－181.

[9] Hariri S，Qu Guangzhi，Dharmagadda T，et al. Impact analysis of faults and attacks in large－scale networks[J]. Security Private Magazine，IEEE，2003，11(1)：49－54.

[10] 诸 晔. 用 ACL 实现系统的安全访问控制[J]. 计算机应用与软件，2005，22(3)：111－114.

[11] 方贤进，李敬兆，姚亚锋，等. 一种校园网的网络安全策略[J]. 计算机技术与发展，2006，16(5)：121－124.

[12] Verma D C，Calo S，Amiri K. Policy－based management of content distribution networks[J]. Network，IEEE，2002，16(2)：34－39.