文章编号:1005-0523(2009)06-0079-04

使用ACL技术的网络安全策略研究及应用

莫林利

(华东交通大学 软件学院,江西 南昌 330013)

摘要:ACL基于包过滤技术,广泛应用于路由器上以提高网络安全性。介绍了ACL技术的基本原理、主要功能以及路由器上ACL的配置和访问原则,并以一个实际的网络拓扑为例,详细分析了如何使用ACL技术来实现网络安全问题的防范,给出了相应安全策略的关键配置代码。

关 键 词:访问控制列表;网络拓扑;网络安全策略;包过滤;Cisco IOS

中图分类号:TP393 **文献标识码**:A

随着计算机网络的迅猛发展和在各行各业的普及,网络中的安全问题也日趋严重。保障计算机网络安全的技术,常用的有访问控制、密码体制、数字签名、防火墙技术以及针对不同层次的网络安全协议等。虽然这些技术都能较好的实现网络安全控制,但是其中有些技术专业要求太高,或者成本较高,并不适合所有的网络。本文主要介绍其中的访问控制列表(Access Control List,简称ACL)技术,通过在路由器或三层交换机上设置合理的ACL策略,可以在一定程度上保护网络中的数据安全,尽可能的降低网络带来的负面影响,而且不会增加经济成本,给网络管理带来极大的方便。

1 ACL技术的基本原理

ACL是Cisco IOS所提供的一种访问控制技术,目前广泛应用于路由器和三层交换机上,部分二层交换机也支持ACL[1,2]。其他厂商的路由器或三层交换机也提供了类似的ACL技术,但是它们的配置方法有些差别,本文主要介绍Cisco ISO支持的ACL技术。ACL使用包过滤技术,在路由器上读取第三层及第四层包头中的信息如源地址、目的地址、源端口、目的端口等,根据预先定义好的规则对包进行过滤,从而达到访问控制的目的[3]。

1.1 ACL的分类

ACL主要分为标准访问控制列表和扩展访问控制列表两种,它同时支持IP协议和IPX协议。标准的IP访问控制列表只根据分组内的源IP地址进行过滤,占用路由器资源较少,应用比较广泛,但是控制级别较低。IP标准访问控制列表的编号一般为1~99。

扩展访问控制列表不仅可以检查数据包的源地址,还可以检查数据包的目的地址、协议类型和TCP/UDP协议族的端口号,具有更大的灵活性和可扩充性[2]。但是扩展ACL会消耗大量的路由器CPU资源,一般来说中低档路由器还是使用标准访问控制列表比较有效。IP扩展访问控制列表的编号一般为101~199。

另外,还有几种比较高级应用的ACL。例如:基于名称的访问控制列表、反向访问控制列表、基于时间的访问控制列表等,使用时可以根据网络安全需要和网络服务效率进行合理选择[4]。

1.2 路由器访问ACL的原则

访问控制列表实际上是一系列安全规则的集合,路由器访问控制列表时,会把访问控制列表中的每一条规则中所定义的IP地址和收到的数据包中的IP地址分别同通配符进行逻辑或操作,如果这两个操作结果一致,则应用此规则,允许或拒绝数据包通过。路由器通常按照ACL列表中的语句顺序来判断执行。

收稿日期:2009-05-20

作者简介:莫林利(1977-),女,河南安阳人,讲师,研究方向为网络工程,网络安全。

数据包只有在跟第一个判断条件不匹配时,才会被交给访问控制列表中的下一个条件判断语句进行比较。如果所有访问控制列表的判断语句都检查完毕还没有找到相匹配的语句,则该数据包被丢弃[3,5]。这是因为 Cisco 的 ACL 技术中最后一个语句默认为 deny any any,而它通常是隐藏的,不需要明显写出来。

1.3 Cisco 访问控制列表的配置原则

在 Cisco 设备上配置访问控制列表时要遵循以下 3 个基本原则[6]:

(1) 最小特权原则:只给受控对象完成任务所必须的最小的权限。

(2) 最靠近受控对象原则:采用自上而下的顺序检查 ACL 列表中的规则,只要发现符合条件的就立即转发,而不用继续检查下面的 ACL 语句。因此,应该把最特殊的测试条件写在 ACL 列表的最上面。

(3) 默认丢弃原则:在 Cisco 设备中,每个访问控制列表的最后一个隐藏规则为 deny any any。而在华为 3COM 设备支持的 ACL 中,最后一个默认规则是 Permit any any。因此不同厂商支持的 ACL 技术在配置时会有一些差别,这些差别对网络安全策略的配置是很重要的。

2 ACL 技术在网络安全中的应用

图 1 是某学院网络拓扑结构的一部分,其中包括教师办公室,服务器机房和学生实验室若干。本网络中全部使用 24 位子网掩码。

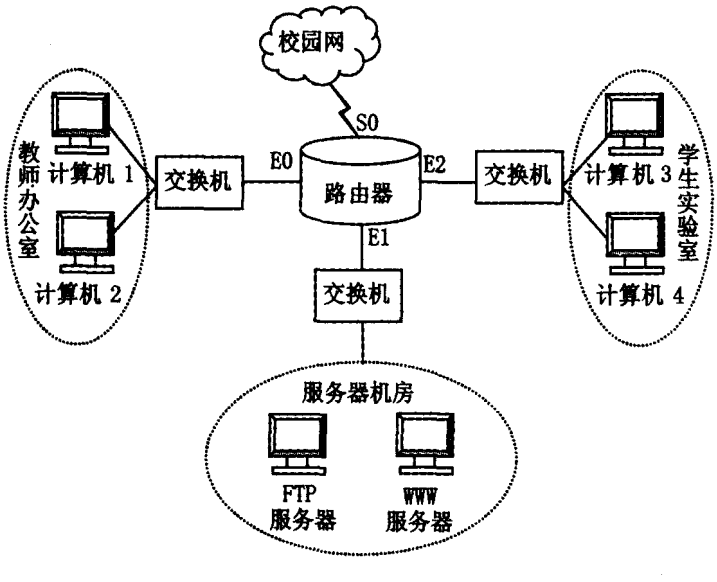

图 1 某学院的网络拓扑结构图

在图 1 中,路由器使用以太网端口 E0 连接到教师办公室(网段为 192.168.1.0),使用以太网端口 E1 连接到学院的服务器机房(网段为 192.168.2.0),使用以太网端口 E2 连接到学生实验室(网段为 192.168.3.0),使用串口 S0 连接到校园网。路由器的 E0、E1 和 E2 端口的 IP 地址分别为 192.168.1.1,192.168.2.1 和 192.168.3.1。计算机 1 的 IP 地址为 192.168.1.11,计算机 2 的 IP 地址为 192.168.1.12,计算机 3 的 IP 地址为 192.168.3.11,计算机 4 的 IP 地址为 192.168.3.12。FTP 服务器的 IP 地址为 192.168.2.11,WWW 服务器的 IP 地址为 192.168.2.12。

根据教师办公室、服务器机房和学生实验室对网络及其数据安全的不同要求,利用 ACL 技术构建了以下的网络安全策略。

2.1 实现网络访问的单向控制

教师办公室(网段为 192.168.1.0)用于教师办公,主机上往往会存放一些试卷等敏感数据,因此不能让学生实验室(网段为 192.168.3.0)访问,但是教师办公室网段可以访问学生实验室的计算机,以便对学生做实验、上课等情况进行管理和监控。

首先在路由器上采用IP标准访问控制列表如下:

```
Router (config) # access-list 1 deny 192.168.3.0 0.0.0.255
Router (config) # access-list 1 permit any
Router (config) # int E0
Router (config) # ip access-group 1 out
```

在路由器上配置成功后,192.168.3.0网段不能访问192.168.1.0网段,但同时192.168.1.0网段也不能访问192.168.3.0网段,原因是在路由器的E0端口的out方向上设置了访问控制策略deny 192.168.3.0 0.0.0.255,它阻止了从192.168.3.0发给192.168.1.0的所有数据包,即使是192.168.3.0给192.168.1.0网段的回复数据包也一样阻止了。由此可见,简单的使用标准访问控制列表还不能解决这个问题。

要实现从192.168.1.0网段到192.168.3.0网段的单向访问控制,采用扩展访问控制列表配置如下:

```
Router (config) # access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255 established
Router (config) # access-list 101 permit tcp any any
Router (config) # int E2
Router (config) # ip access-group 101 in
```

该策略的原理是当TCP连接已经建立时,在路由器的E2端口的in方向上检查数据包,如果它是表示确认的数据包即可通过,而如果是从192.168.3.0向192.168.1.0网段发起TCP连接的数据包,则它不表示确认数据包,因此拒绝通过。这样设置后,学生在实验室就不能任意访问教师计算机上的试卷等敏感资料,而教师计算机依然可以管理学生实验室的上课和上机情况。

2.2 禁止或允许部分网络服务

实验室一旦连接了校园网,就可以访问很多资源,包括电影之类。但是实验室是为学生提供做实验、学习的场所,在上课期间不允许学生下载电影或在线观看。在图1中,假设绝大部分电影之类的资源放在校园网的192.168.2.0网段的FTP服务器上,因此要拒绝学生实验室192.168.3.0网段访问192.168.2.0网段的FTP服务,但是依然可以正常访问WWW服务。可以采用以下的ACL配置策略实现该要求:

```
Router (config) # access-list 102 permit tcp 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255 eq www
Router (config) # access-list 102 deny tcp 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255 eq ftp
Router (config) # access-list 102 permit ip any any
Router (config) # int E1
Router (config) # ip access-group 102 out
```

在学生实验室,象QQ游戏之类的网络应用也是不允许学生使用的,可以采用同样的原理来禁止该项服务。首先需要查找到在因特网上提供QQ游戏的服务器的IP地址,然后采用ACL命令来禁止学生实验室网段192.168.3.0和这些IP地址的服务器之间的网络连接。

2.3 禁止某台主机的通信

局域网受病毒攻击是不可避免的,一旦局域网内有一台计算机感染病毒,就有可能影响整个局域网内的通信,严重时可能导致网络瘫痪。虽然不能彻底将病毒拒之门外,但是可以在尽量防毒基础上,及时检测病毒并对有毒主机采取隔离措施以保护网络。

假设学生实验室的计算机4(IP地址为192.168.3.12)主机感染了病毒,正在向局域网内的其他主机疯狂发数据包,那么可以采用以下ACL策略限制该主机的数据传输,从而阻断病毒向其他网段的传播,将病毒对网络的影响降到最小:

```
Router (config) # access-list 2 deny 192.168.3.12 0.0.0.0
Router (config) # access-list 2 permit any
Router(config) # int E2
Router(config) # ip access-group 2 in
```

2.4 保护重要端口免受病毒攻击

操作系统开放了一些端口,例如135,136,137,138,139,445等。病毒攻击原理就是向这些开放端口发

送大量数据,使所有操作系统资源和网络资源耗尽,最终使得网络无法向合法用户提供正常的服务[7]。使用ACL防范病毒攻击的策略如下:

```
Router(config) # access-list 103 deny tcp any any eq 135
Router(config) # access-list 103 deny udp any any eq 135
Router(config) # access-list 103 deny ip any any eq 135
Router(config) # int S0
Router(config) # ip access-group 103 in
```

以上策略是以135端口为例,其他端口的配置策略相同,限于篇幅不再详述。在路由器上限制对135端口基于TCP、UDP和IP协议的访问,从而禁止病毒通过135端口攻击内网。当然,该策略同时也禁止了135端口的其他正常使用。

3 结语

通过对路由器配置以上的ACL策略,对内部网络构建了基本的网络安全体系,在一定程度上可以提高网络的安全性。但是ACL是使用包过滤技术来实现的,过滤的依据仅仅只是第3层和第4层包头中的部分信息,而且如果ACL策略运用不当还可能造成网络资源的浪费,降低网络服务效率。因此,必须结合网络的实际情况和设备的实际支持功能,在网络中合理的、适当的使用ACL技术,既保护了网络安全,又充分发挥了网络服务效率。

参考文献:

[1] 唐子蛟,李红蝉.基于ACL的网络安全管理的应用研究[J].四川理工学院学报(自然科学版),2009,22(1):48-51.
[2] 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,2004,21(4):89-92.
[3] 王 芳.路由器访问控制列表及其应用技术研究[D].郑州:解放军信息工程大学,2007.
[4] 陈 琳,朱绍文,陈绪君,等.新型Access-List技术应用研究[J].计算机应用,2002,22(8):69-71.
[5] 胡海璐,陈曙晖,苏金树.路由器访问表技术研究[J].计算机科学,2001,28(4):94-96.
[6] 王 芳,韩国栋,李 鑫.路由器访问控制列表及其实现技术研究[J].计算机工程与设计,2007,28(12):5 638-5 639.
[7] 陈卫荣.Cisco路由器访问控制列表配置实现第一道网络安全屏障[J].武麦学院学报,2008,27(5):60-64.

Research and Application of Network Security Policies with ACL

MO Lin-li

(School of Software, East China Jiaotong University, Nanchang 330013, China)

Abstract: ACL, one of packet-filtering technologies, is widely used in the router to improve network security. The paper firstly gives a brief introduction of concept and working principle, main function, collocation and access method of the access control list. Then the paper takes a actual network topology as an example to analyze in detail how to safeguard the network security with ACL technology, and give the key codes of corresponding network security policies.

Key words: access control list; network topology; network security policies; packet filtering; Cisco IOS

(责任编辑:王建华)