文章编号:1005－0523(2004)04－0089－04

基于ACL的网络层访问权限控制技术研究

范 萍[1],李罕伟[2]

(华东交通大学 1.信息工程学院; 2.现代教育技术中心 江西 南昌 330013)

摘要:阐述了ACL基本原理,简单配置方法,用一些实例说明如何实现使用ACL进行网络层访问权限控制,提高网络整体性能和安全.

关 键 词:ACL;网络层;权限控制
中图分类号:TU317+.1 **文献标识码**:A

1 日益严重的安全威胁

目前,学校越来越依赖网络才能更好地运转,比如网络办公、网上新闻信息发布、网络辅助教学、网络远程教育等等.因此,学校遭受网络攻击的风险也越来越高.网络攻击和病毒破坏不但会中断关键运作过程,还会导致办公效率降低,信息传递不畅,网上教学无法进行.

目前互联网上最猖獗的网络威胁主要包括:

1) DDOS(拒绝服务)攻击——最常见的攻击方式,通过用于在互联网上下载文件的程序发动.其目的是过度占用网络、操作系统或应用上的资源,使学校网络无法提供正常的服务.如红色代码、Nimda等.

2) 病毒、木马和蠕虫——终端用户的PC尤其容易遭受病毒和木马攻击.如前段时间的"冲击波"病毒,曾一度给全世界的网络造成影响.

3) 应用层攻击——利用操作系统漏洞,接入具有较高管理权限的计算机,从而进行破坏活动.

2 ACL简述

ACL(Access Control List)是Cisco IOS所提供的一种访问控制技术,初期仅在路由器上支持,近些年来已经扩展到三层交换机,部分最新的二层交换机如2950之类也开始提供ACL的支持.只不过支持的特性不是那么完善.在其它厂商的路由器或多层交换机上也提供类似的技术,不过名称和配置方式都可能有细微的差别.本文所有的配置实例均基于Cisco IOS的ACL进行编写.

基本原理: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协议、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.

功能:网络中的节点分资源节点和用户节点两大类,其中资源节点提供服务或数据,用户节点访问资源节点所提供的服务与数据.ACL的主要功能就是一方面保护资源节点,阻止非法用户对资源节点的访问,另一方面限制特定的用户节点所能具备的访问权限.

配置ACL的基本原则:在实施ACL的过程中,

收稿日期:2004－03－10
作者简介:范萍(1979－),女,江西进贤人,助教.

应当遵循如下两个基本原则.

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:所有的网络层访问权限控制

局限性:由于 ACL 是使用包过滤技术来实现的,过滤的依据又仅仅只是第三层和第四层包头中的部分信息,这种技术具有一些固有的局限性,如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 end to end 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.

3 ACL 的详细配置方法

3.1 ACL 的基本格式

标准访问控制列表:

access－list access－list－number { **permit** | **deny** } {source source－wildcard | **any**}

扩展访问控制列表:

access－list access－list－number { **permit** | **deny** } {protocol | protocol－keyword } {source source－wildcard | **any** } {destination destination－wildcard | **any** } [protocol－specific options] [log]

表 1 "access－list"命令选项

选 项	描 述
access－list－number	标志该条目所属的访问控制列表.标准访问控制列表编号是:1～99;扩展访问控制列表编号是:100～199
permit	deny	说明如果与测试条件匹配时将产生的结果."允许"让数据包进入或者外出这个接口."拒绝"是扔掉这个数据包并向源发送一个 ICMP 消息
Protocol	说明要匹配的协议类型.选项包括 ip、tcp、udp、icmp、igrp、eigrp、ospf、nos,和 0～255 的任一个号码.要匹配所有协议,使用关键字"ip"
source 和 destination	源和目的地的 IP 地址
source－wildcard 和 destination－wildcard	说明要匹配地址比特数的通配符标志."0"表示要准确地匹配这个比特;"1"表示这个比特可以是任意比特
Log	产生与这个条目相匹配的数据包信息记录.

3.2 ACL 的特性

1) 标准 ACL 的测试条件只是基于源地址;

2) 扩展 ACL 的测试条件包括协议类型、源地址、目的地址、应用端口和会话层信息;

3) 对访问控制列表的处理是自上向下的.一旦在访问控制列表中找到了匹配,就停止处理,并且根据访问控制列表中的命令语句,允许或拒绝数据包;

4) 在每个访问控制列表的末尾有一条对所有条件的隐含拒绝语句.如果在访问控制列表中没有发现匹配,那么它最终将与这条隐含语句相匹配;

5) 访问控制列表在被应用到对应端口以前,将不具任何意义,对数据流不产生控制.

3.3 如何将 ACL 应用到端口

访问控制列表建立以后,便可被应用到接口以阻止数据流进入或离开接口.可以通过"ip access－group access－list－number [in | out]"命名将访问控制列表应用到接口上.

如图 1 中所示的访问控制列表进行如下的工作:

1) 允许来自任何主机的所有 TCP 数据流到达子网 192.168.2.0;

2) 如果应用类型是 SMTP(邮件),则允许所有设备到达主机 192.168.1.2

3) 允许应用类型为域名服务(DNS)的 UDP 数据包;

4) 允许 ICMP 回声和回声应答(ping);

5) 拒绝所有其它数据流.

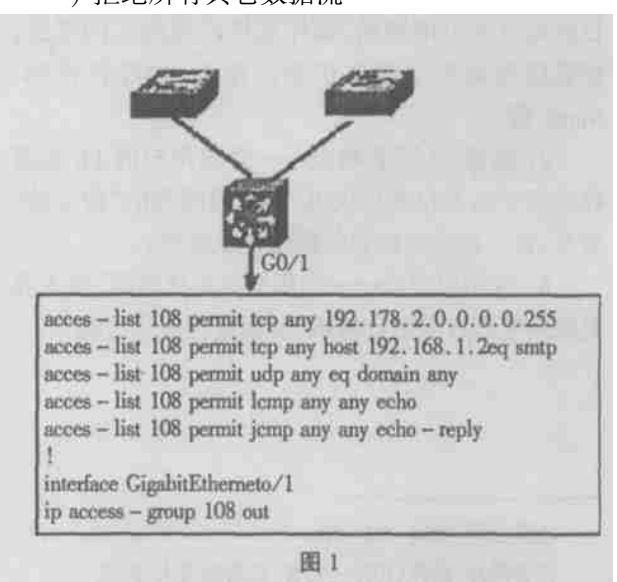

图 1

4　根据校园网络应用进行安全访问控制

4.1　关闭常见易遭受攻击端口

由于操作系统本身具有的漏洞,给许多病毒和网络攻击提供了可乘之机,虽然操作系统都会及时提供补丁,但对于大多数用户来说,并不具备提高自己系统安全性的意识或技术,因此对于常见易遭受攻击端口进行封堵,就显得尤为重要.如下控制列表 access－list 110 就是专门针对常见漏洞端口设计的,将其应用在边界路由上,便能够抵御来自 Internet 的大部分常见攻击.

访问控制列表 access－list 110 及其作用:

1) access－list 110 deny　tcp any any eq 445
用于控制蠕虫的扫描和感染;

2) access－list 110 deny　tcp any any eq 5800;

3) access－list 110 deny　tcp any any eq 5900
用于防止受感染的系统被远程控制;

4) access－list 110 deny　tcp any any eq 6667;

5) access－list 110 deny　tcp any any eq 6588.
用于控制受感染的系统与聊天服务器的通信;

6) access－list 110 deny　udp any any eq 1434
用于控制 Slammer worm;

7) access－list 110 deny　255 any any;

8) access－list 110 deny 0 any any;
用于控制 IP Protocol 为 255 和 0 的流量.

9) access－list 110 permit ip any any

4.2　针对服务器的应用设计 ACL

通常网络服务主要集中于 Web、DNS、Mail、Ftp,这些服务器并不是所有端口都需要用到,因此我们一般都会在服务器上关闭不用的端口,以减少服务器的安全漏洞.但是,对于所有的攻击数据包,服务器都必须做出处理——接收还是丢弃?如果遭遇像 SYN Flood 一样的攻击,即使服务器本身并不存在安全问题,但服务器将由于大量的数据处理而过载.所以,这时我们就需要使用 ACL 将攻击拒绝于到达服务器之前.这里以 IP 为 192.168.2.10 的 Web 服务器为例,使用如下访问控制列表:

access－list 112 permit tcp any host 192.168.2.10 eq 80

因为 Web 服务只需要 TCP 80 端口提供服务,因此将网络上到 Web 服务器的 TCP 80 以外的访问全部拒绝,这样 Web 服务器便可以安全高效地提供服务.对于其他的服务器,使用相同的方法进行处理,这个服务器的安全将会更上一层楼.

4.3　交换路由设备安全控制

交换路由设备本身也相当于一台运行着的主机,也有其自己特有的操作系统.(本文研究的 Cisco 交换路由设备,使用的就是其专有的操作系统 IOS)也就是说,交换路由设备本身也存在被攻击的可能,因此我们必须针对交换路由设备作一些必要的安全访问控制.

目前,针对交换路由设备的安全控制主要有以下两方面:

1) 关闭交换路由设备的 HTTP 服务,采用如下指令:

no ip http server

HTTP 服务是 Cisco 交换路由设备提供的 Web 管理服务,但其存在一些安全漏洞.

2) 设计如下访问控制列表,限制到交换路由设备的 Telnet 操作

access－list 1 permit host 192.168.5.55

line vty 0 4

access－class 1 in

这里 line vty 0 4 代表我们使用 Telnet 登录交换路由设备时使用的几个虚拟接口,将访问控制列表 access－list 1 应用到它们上面以后,只有从主机 192168.55 发起的 Telnet 请求才会被接受.

4.4　针对网络最新安全公告及时更新 ACL

随着操作系统最新漏洞的发现,必将出现越来越多的病毒,而针对网络的自动传播的蠕虫类更是当前网络病毒发展的热点.因此,作为网络管理人员,必须时刻关注权威网站的安全公告,并通过现有设备尽可能的采取保护措施.

比如 8 月份爆发的冲击波,对全世界网络均造成了不同程度的阻塞.如果网络管理员了解到了这一情况,就可以根据病毒传播所使用的端口和协议,在交换路由设备上有针对性地设置访问控制列表(ACL)进行网络层的访问权限控制,便可将其拒之门外,保证内网的安全.

在网络世界里没有绝对的安全,因此,我们必须时时提升自己的安全防护能力,才能更好地开展网络办公和网络教学.

5　结束语

使用 ACL 进行网络访问权限控制,是目前主流交换路由设备的必备功能,可以有效地提升网络的

安全等级.但是,毕竟交换路由设备的主要功能是数据的交换和路由,过多的使用 ACL 将可能消耗系统的大量资源,进而影响交换路由设备的数据交换和路由性能.这样,就等于是牺牲网络运行效率来提高网络安全性.因此,如果需要进行较大规模的访问权限控制及数据安全过滤,最好选择专门的硬件防火墙.综上所述,笔者认为,网络管理员必须充分了解网络的实际应用状况,网络设备的功能和处理能力以及网络安全相关的最新信息,结合实际情况,在网络中合理、适当地使用 ACL 访问控制列表进行网络层访问权限控制,网络性能将得到大幅提升,从而让 ACL 这一先进技术的优势得以充分发挥.

参考文献:

[1]李逢天,张帆,译.Karen Webb. 组建 Cisco 多层交换网络[M].北京:人民邮电出版社,2000.

[2]赵 刚,等译.Rajesh Kumar Sharma, NIIT. Cisco 网络安全宝典[M]. 北京:电子工业出版社,2002.

Research on Technique to Control Access to Network Layer Based on ACL

FAN Ping[1], LI Han-wei[2]

(1.School of Information Eng.;2.Modern Educational Technology Center, East China Jiaotong University, Nanchang 330013, China)

Abstract: This paper expatiates on the theory of ACL and a simple method to configure it and then explains the method how to improve capability and security of network using some instances.

Key words: ACL; network layer; access control

(上接第 44 页)

[23] Miyake M etc. The correlation between photo-electrochemical cell reactions and photocatalytic reactions on illuminated rutile .Bull. chem..Soc.Jpn, 1977, 50(6):1492-1496.

[24] 戴遐明.半导体氧化物超细粉末对 Cr(Ⅳ)的光催化还原研究[J].环境科学.1996,17(6): 34.

[25] Frank S N, Bard A J. Heterogeneous photocatalytic oxidation of cyanide ion in aqueous at power.[J].Am. Chem.Soc., 1977, 99(1):303-304.

[26] Bhakta D, Shukla S S, Chandrasdeharaish M S. A novel photocatalytic method for detoxification of cyanide wastes[J]. Environ[J]. Sci. Technol, 1992, 26(1992): 625.

[27] Serpone N, Ah-You Yk, Tran T P. AM1 siumlated sunlight photoreduction and elimination of Hg(Ⅱ) and CH_3Hg(Ⅱ)chloride salts from aqueous suspensions of titanium dioxide [J]. Solar Energy, 1987, (39):491.

Development of TiO_2 Photocatalytic on Pollutants of Wastewater Treatment

FENG Gui-zhen, JIANG Li-wen

(School of Civil Engineering and Architecture East China Jiaotong University, Nanchang 330013, China)

Abstract: The development of multiphase photocatalytic technology used in wastewater treatment has been paid more attention by environmentalist.This article summarizes the mechanism of TiO_2 photocatalyst and development of photocatalytic applications on wastewater treatment.

Keywords: TiO_2; photocatalysis; pollutant degradation; wastewater