路由器访问表技术研究

On Router Access Control List Technology

胡海璐　陈曙晖　苏金树

（国防科技大学计算机学院　长沙410073）

Abstract　In the paper, the principium of IP Acess Control List has been presented. Also the development trend of Access Control List has been discussed: Dynamic Access Control List, Time Based Accesslist, Reflexive Access Control list, Context Based Access Control.

Keywords　Acess conrtol list, Message filtering, Matching

1　引言

作为一个公共的网络，Internet是缺乏安全性的，因此对内部网而言，必须采取一定的措施，保证内部私有信息的安全。路由器工作在网络层，其主要工作是转发IP报文，它是内部网和Internet的衔接处，所有内部网络到Internet的报文都要流经路由器，尽管路由器非常灵活，并拥有高度的用户配置能力，但它们一般并不查看所传输的数据，也不提供认证远程用户，加密数据传输的流量，或执行代理的功能。因此，必须通过编写路由器的访问表来实现分组过滤，作为防止攻击的第一道防线。

本文将讨论访问表技术在路由器安全中的作用。

2　访问表概述

保证安全有许多手段，其中最为重要的是使用报文过滤来控制报文流进网络。通过检测报文头部的信息来防止特定的报文进出某一个网络的技术称为“报文过滤”。访问表的主要功能就是进行报文过滤。

访问表是根据匹配规则和报文来允许或拒绝报文流的排序表。访问表语句既可以允许报文的流动，又可以拒绝报文的流动，用于允许或拒绝报文的标准是基于报文自身所含的信息。通常这些信息只限于第三层和第四层报文头中所包含的信息。有一种称为基于上下文的访问控制(CBAC)，能够基于应用层信息过滤报文。

传统的访问表报文过滤策略是基于IP报文的源

胡海璐　硕士生，主要研究方向为计算机网络；陈曙晖　讲师，主要研究方向为计算机网络；苏金树　教授，主要研究方向为计算机网络。

有了可行的机制，但更需要好的“策略”，即对系统的Capability权限应做合理的全面设计和规划。

(2)本文机制的原型只实现了用户、进程和程序GET、SET的Capability接口函数，还需完成文[1,2]定义的其它接口函数。

(3)实现其它安全机构：ACL、MAC、Audi、IL，以及它们之间的交互。

(4)在尽量减少开销和复杂度的前提下，补充开发实际有用的Capability权限升降机制。

参考文献

1　Portable Applications Standards Committee of the IEEE Computer Society. Draft Standard for Information Technology-Portable Operating System Interface(POSIX)-Part 1: System Application Program Interface (API)-Amendment #: Protection, Audit and Control Interface [C Language]. New York: the Institute of Electrical and Electronics Engineers, Inc., 1997. 163～194

2　Technical Committee on Operating Systems and Application Environments of the IEEE Computer Society. Draft Standard for Information Technology-Portable Operating System Interface (POSIX)-Part 2: Shell and Utilities-Amendment #: Protection and Control Interface. New York: the Institute of Electrical and Electronics Engineers, Inc., 1997. 25～33

3　Morgan A G. DEPARTJIMENT OF DEFENSE STANDARD: DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (Aka. The Orange Book). DoD 5200. 28-STD; Supersedes; CSC-STD-001-83, dtd 15 Aug 83; Library No. S225,711, December 1985

4　Sutton S A. TST. The Hewlett-Packard Compartmented Mode Workstation HP-UX CMW Volume Ⅰ: Administration Tutorial. Urbara, Illinois: Trusted Systems Training, Inc., 1995, chapter 3, chapter 4

地址和目的地址或IP报文的源端口和目的端口对IP报文进行过滤，通过将定义的规则应用到路由器的不同端口及信息的流向（流出或流入）可以严格地控制流经路由器的所有报文，过滤掉认为有损安全的报文。

3 访问表结构设计

访问表的主要功能是进行报文过滤，一个报文过滤是一个基于不同标准、允许或拒绝报文的语句排序表。用来允许或拒绝报文的标准通常为第三层的地址（或）第四层的端口信息。从功能上分析，大致上访问表应当包含三个部分：①定义访问表的编号；②访问表需要执行的动作；③访问表匹配报文的标准。

首先，访问表是由一系列规则所组成的，同一个路由器上可以有多条访问表，因此，应该给访问表分配一个指定范围内的号码，用于未来对它的引用。

其次，对匹配访问表的报文要执行何种动作，是允许报文通过还是拒绝报文？

最后，匹配报文的标准定义了用户需求。它应当包含描述源子网和目的子网的第三层IP地址信息或第四层的端口信息。要描述子网就必须有子网的IP地址及其子网掩码，端口信息则涉及到端口号的范围。访问表可以用于多种协议的过滤，如IP、IPX、AppleTalk、DECnet、VINES及XNS等，这样在设计访问表时，还要考虑增加一个标志协议类型的选项。

考虑到访问表在功能上的可扩展性，还可以增加一个备用的选项，用来记录日志、优先级或Tos之类的辅助信息。

根据以上的分析，访问表形式可设计为：

access-list [access-list number][permit|deny][protocoll][soucce-ip source-netmask][destination ip destination-netmask][port range]

其中，assess-list number表示访问表编号，permit|deny表示对匹配的报文执行的操作，protocol表示过滤的协议类型，soucce-ip source-netmask表示源子网信息，destination ip destination-netmask表示目的子网信息，port range表示过滤的端口信息。

4 访问表工作流程

访问表是有顺序的表，它们被从头到尾进行匹配。如果找到了一个匹配项，则访问表处理过程结束，且不再考虑其他更多的项。图1的流图说明了这个过程。

5 访问表未来的发展方向

传统的访问表存在很多局限性，它们在进行报文过滤的时候只能翻译最高到第四层的报文信息，而且不能保留已存在连接的状态信息等。随着网络的发展，客观上要求访问表能过滤通用应用程序的高层信息，更有效地保证网络的安全。下文，将讨论访问表未来的几个发展方向：动态的访问表，基于时间的访问表，反访问表以及基于上下文的访问控制（Context Based Access Control，CBAC）。

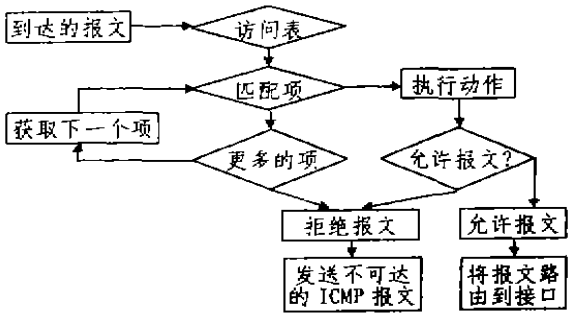

图1 访问表工作流程图

5.1 动态访问表

动态访问表是可以在用户认证过程中进行动态开启的访问表。动态访问表允许在传统的OIP访问表中加入动态表项。用户可能要打开一个到路由器的Telnet会话，此时需要对用户进行认证。一旦用户被认证，路由器将关闭Telnet会话，并在向内的访问表中增加一个动态的表项，该表项将允许来自用户工作站的报文。如果空闲的时间过长，或连接超时，表项会被动态地清除。用户的授权可以通过路由器自身的用户数据库，或者TACACS+、Radius服务器进行。管理员还可以对所有用户指定一个通用的口令进行认证。

注意，路由器在认证之后立即关闭了连接，并将一个动态的表项增加到了访问表中。

尽管动态访问表在传统IP访问表的基础上提供了一些重要的增强特性，但还是有其固有的局限性。首先，没有办法可以使管理员为不同用户提供不同类型的访问。而且，允许外部的主机在访问表中建立动态的表项会带来潜在的安全问题，因为外部网络可以通过嗅探（sniff）网络而捕获到登录信息。通常的Telnet会话采用明码传输登录信息，这意味着攻击者可以被动地（简单地）收集到这些信息。这种攻击可以通过首先控制ISP处的某台机器，然后在其上安装嗅探器（sniffer）软件而进行。

因此，当允许来自Internet的用户可以通过访问路由器而建立动态表项时，一定要谨慎考虑。如果要使用动态访问表，建议只对特定IP地址和特定协议开放。如果某个黑客能够在合法用户登录期间嗅探到用户ID和口令，他就能在路由器上建立与合法用户同样的表项，并利用这个表项进入内部网络进行进一步的攻击。因此，使用动态访问表时，一定要小心。

5.2 基于时间的访问表

基于时间的访问表可以让管理员基于一天中的不同时间和一星期的不同天而建立不同的安全策略。它

允许网络管理员对流入和流出网络的数据进行附加的控制。这种基于时间的数据流过滤实现方法使得网络管理员对组织中的策略和过程更具有敏感性。例如，某些组织可能希望所有的或特殊的雇员在通常的业余时间之后可以进行 Web 冲浪。基于时间的访问表使得满足组织的这种需求变得容易。它的另一个应用是在不同的时间段内通过服务类型(type of service，TOS)域改变数据流。还可以使用基于时间的访问表来控制日志消息，以记录不同时间段的行为。

显然，基于时间的访问表要求路由器拥有正确的时间。可以使用 NTP 将它们的时钟同步到一个可靠的时钟源上，Cisco 路由器可以通过 ntp master 命令，让路由器拥有可靠的时钟。

5.3 反访问表

反访问表提供了一种保留已存在连接状态信息的方式。反访问表通过建立动态的、临时的表项可以判断一个报文是否为一个已存在连接的一部分。

当一个新的 IP 对话从内部网络发往外部网络时，反访问表可以被触发。反访问表产生一个新的、临时的开启表项。如果流量是原有会话的一部分的话，新的表项可以允许流量进入网络。传统的访问表没有方法可以判断一个报文是否为一个已存在连接的一部分。反访问表通过建立动态的、临时的表项可以弥补这个不足。

当一个新的 IP 对话从内部网络发往外部网络时，反访问表可以被触发。反访问表产生一个新的、临时的开启表项。如果流量是原有会话的一部分的话，新的表项可以允许流量进入网络，这个被创建的临时表项拥有以下特征：

·表项总是 permit 的。

·表项指定了与原来的向外报文相同的协议(例如，TCP、UDP、ICMP 或 IP)。

·新的表项交换源和目的 IP 地址。

·新的表项还交换源和目的端的上层端口号(对 ICMP 而言，使用类型号)。

·如果会话被关闭，或空闲超时，则表项将自动清除。只有 TCP 对话可以通过监视报文中的 FIN 或 RST 位而主动关闭。UDP 等其他协议必须空闲超时才会被关闭。

本质上，反访问表在一个已存在的访问表中建立了"镜像"或称为"反向的"表项，这些表项使得一个已存在连接的报文可以通过访问表。

反访问表是强有力的，但它们有一个主要的缺点。许多协议并不使用一个固定的端口号。例如，FTP 在对话期间就使用多个端口号。FTP 还会从服务器发出一个到源主机的连接。反访问表不能解决这类应用程序所遇到的问题。因此，反访问表只适应于处理只使用单个的、静态的端口的应用程序，并且要求该端口在一个会话期间不会改变。

5.4 基于上下文的访问控制(CBAC)

CBAC 在概念上与反访问表很相似，它可以检测向外的会话，并临时性地允许返回的流量，所不同的是它还可以基于上层信息检测和安全地处理大量应用程序，CBAC 包含了一些附加的智能特性，它可以通过应用层协议的信息，学习 UDP 和 TCP 会话的状态来过滤报文，这个特征使得它可以支持通过客户机/服务器进行协商的多通道应用程序，如 FTP。

CBAC 是在报文离开指定的接口时进行报文检测。报文中包含的信息，如 IP 地址和端口号等，被保留在报文"状态信息"表中。CBAC 使用状态表来在访问表中建立临时的表项，以允许返回的流量。CBAC 检测特定协议的应用层信息，以保证让正常的返回流量可以通过。例如，CBAC 可以监视向外的 FTP 会话，并允许 FTP 服务器发往原客户机的连接得以建立。CBAC 能够辨别出 FTP 应用程序的行为，并能在路由器访问表中建立必要的表项。CBAC 执行上述其他协议的功能时与 FTP 相似。但其局限性是：

·CBAC 只检测 TCP 和 UDP 报文，其他的 IP 流量(如 ICMP)应该使用传统的 IP 访问表进行过滤。

·以路由器作为源地址和目的地址的报文不被 CBAC 检测。

·如果同时配置了加密和 CBAC，CBAC 将不能准确地检测加密报文的内容。在这种情况下，唯一能够检测的多通道协议是 Stream Works 和 CU-SeeMe。CBAC 应该配置成只检测这类应用程序和普通的 TCP/UDP 会话。

·CBAC 对每个连接大约使用600个字节的存储空间，以记录其状态信息。而且，检测过程中可能发生一些附加的处理过程。

小结 本文主要讨论了 IP 访问表技术的工作原理，实际中可以根据协议的不同选用不同类型的访问表来允许或拒绝信息通过一个或多个路由器接口。

访问表只是保护网络安全的第一层，尽管在传统的访问表基础上它有很多增强特性，但是它仍然存在局限性，例如它不能够认证数据是否未经修改。认证过程要求加密报文的信息域以隐藏其内容。它只能提供有限的安全防护，完善的安全措施仍要由专门的网络安全设备来完成。

参 考 文 献

1 Held G，Hundley K. Cisco Security Architectures
2 Cisco Systems 公司著，希望图书创作室译. Cisco IOS 12.0参考库—接口配置技术
3 Cisco Systems 公司著，希望图书创作室译. Cisco IOS 12.0网络安全解决方案