文章编号：2096-1472(2021)-06-17-03
DOI:10.19644/j.cnki.issn2096-1472.2021.06.004

时间访问控制列表实施服务器安全访问

汪海涛，王 磊，戴宏明

(广东科贸职业学院信息与自动化学院，广东 广州 510430)
✉327992570@qq.com; 26568372@qq.com; 1355369191@qq.com

摘 要：在计算机网络中，服务器对不同的客户端提供不同时间规定的访问服务，其他时间禁止客户端访问，进行服务器数据自动备份，提高了服务器的安全性和稳定性。针对该需求，可以在连接服务器的三层设备上启用时间访问控制列表，定义好服务器允许访问的时间规则，将该规则应用到扩展访问控制列表，并把列表绑定到相应的端口。针对某一局域网网络连接Internet结构，论述时间访问控制列表技术，分析时间访问控制列表的特点和应用方法，最终实现服务器在时间策略上的安全访问。

关键词：时间访问控制列表；服务器；网络；安全
中图分类号：TP393 **文献标识码**：A

Implementation of Server Security Access based on Time Access Control List

WANG Haitao, WANG Lei, DAI Hongming

(*College of Information & Automation*, *Guangdong Polytechnic of Science and Trade*, *Guangzhou* 510430, *China*)
✉327992570@qq.com; 26568372@qq.com; 1355369191@qq.com

Abstract: In computer network, server provides different clients with access services specified at different times. Clients are prohibited from accessing at other times when server automatically backs up data to improve its security and stability. To meet this need, time Access Control List (ACL) is enabled on the three-tier device connected to the server and the defined time rule for accessing server is applied to the extended access control list which is bound to the corresponding port. This paper discusses the technology of time Access Control List, analyzes characteristics and application methods of the time Access Control List, and finally realizes secure server access in the time strategy for Internet structure of a certain LAN (Local Area Network) network connection.

Keywords: time Access Control List; server; network; security

1 引言(Introduction)

Internet和Intranet系统中，某些特定的服务器对客户端仅提供特定时间的访问服务，其他时间禁止客户端的访问，这样可以有效地提高服务器的安全性。通常在计算机网络服务器连接的三层设备(例如三层交换机或路由器)上启用时间ACL，定义好服务器允许访问的时间规则，将该规则应用到扩展访问控制列表中，最后启用三层设备的防火墙功能，把扩展控制列表的列表号绑定到通往服务器的相应端口上[1]。这样，计算机网络中的客户端访问服务器的时候，数据包经过该三层设备的相应端口，防火墙就对比访问的时间是否满足定义的时间规则，如果满足就允许访问服务器，否则就拒绝访问服务器[2]。

2 时间访问控制列表的概念(The concept of time Access Control List)

我们首先来了解ACL的概念：ACL(Access Control List)即访问控制列表；然后来了解时间ACL的概念：时间ACL根据制定的时间规则执行访问控制。计算机网络管理者使用时间ACL，首先创建一个时间范围，指定服务器被允许访问的时段，或者是数据包被允许通过的时段[3]；然后命名该时间范围，并将该名称应用在对应的扩展访问控制列表中。

基金项目：广东省教育科学“十三五”规划2020年度研究项目(2020GXJK304)；广东省普通高校特色创新类项目(2019GKTSCX038)；全国工业和信息化职业教育教学指导委员会项目(GXHZW20201101，GXHZW20201602).

时间ACL相对标准ACL和扩展ACL具有很多优点：

⑴数据包时间访问设定为网络管理者提供了较好的控制权[4]。

⑵网络管理者能够较好地掌握日志消息。

3 时间访问控制列表定义时间的方法(The method of defining time in time access control list)

时间访问控制列表定义时间的方法有以下两种：

⑴相对时间范围

相对时间范围是按照星期来定义时间规则的，命令格式为：

time-range time-name start-time to end-time days

time-range是命令关键词，后面的参数含义解释如下：

time-name：时间范围名，通常是英文字母和数字组合的字符串。

start-time to end-time：开始时间和结束时间，其格式是[小时:分钟] to [小时:分钟]。

days：表示一个星期的某一天或者是某几天，也可以是工作日(周一到周五)或者是非工作日(周六到周日)。从周一到周日对应的关键字分别是Mon、Tue、Wed、Thu、Fri、Sat、Sun。days可以用周一到周日的这些关键字中的一个或者几个的组合来表达。为了方便，有的路由器、三层交换机也用数字代表，0表示星期日，1表示星期一，……6表示星期六。用其中一个数字或者几个数字组合代表相应的星期几。其他的特殊关键字有：working-day代表工作日，即周一到周五；Daily代表一周七天，每一天；off-day代表周六和周日周末两天[5]。

例如，现在制定一个时间规则，要求从每周四下午3点到每周五上午10点客户端可以访问服务器，其他时间不可以访问，可以这样配置时间范围：

time-range aaa 15:00 to 00:00 Thu

time-range aaa 00:00 to 10:00 Fri

⑵绝对时间范围

绝对时间范围是按年月日具体的某一天来定义的[6]，其命令格式如下：

time-range time-name from time1 date1 [to time2 date2]

time-range是命令关键词，其他参数含义和上一段参数含义类似，下面举例说明。例如，现在制定一个时间规则，要求从2021年2月1日早上9点半开始生效，2021年2月12日晚上8点停止生效，这一时间范围客户端可以访问服务器[7]，其他时间不可以访问，可以这样配置：

time-range bbb from 09:30 2021/2/1 to 20:00 2021/2/12

4 时间访问控制列表方案规划和实现 (Planning and implementation of time access control list scheme)

4.1 方案建设原则和目标

项目方案采用时间ACL应用在相应扩展控制列表技术中。项目拓扑结构中的内网有一台Web服务器对内网用户和Internet中的所有客户端提供网页浏览服务。Web服务器对内网用户提供访问服务的时间是周一到周日的8:00到20:00，对Internet用户提供访问服务的时间是周一到周五的9:00到18:00，其他时间为服务器的数据备份时间[8]。

4.2 方案的总体规划

系统方案结构为企业内部网接入Internet，RouterA是内网的出口路由器，RouterB、RouterC为Internet的两台路由器，SwitchA为内网的核心交换机(三层交换机)。Web服务器和核心交换机相连，PC0为Internet的客户端和RouterC相连，PC1、PC2是内网的客户端。PC1是vlan10的客户端，PC2是vlan20的客户端，PC1、PC2和二层交换机相连。整个系统的拓扑图如图1所示。

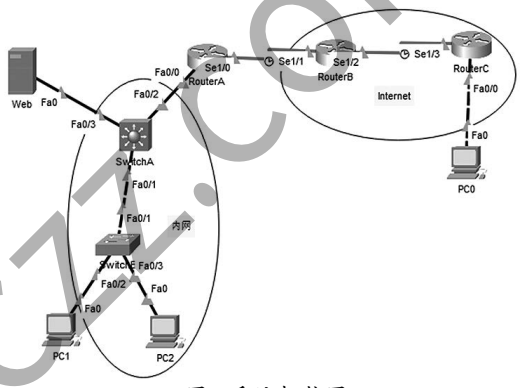

图1 系统拓扑图

Fig.1 System topology

4.3 方案的实现

4.3.1 整个网络系统连通的配置

首先，配置好网络拓扑系统的IP地址、PC客户端和Web服务器的IP地址和默认网关；配置好路由协议和出口路由器的NAT；配置Web服务器的静态NAT映射一个对外IP地址，让内网可以访问外网，外网的客户端通过静态NAT映射的对外IP地址可以访问Web服务器。

网络系统连通性配置如以下代码所示：

```
RouterA(config)#router rip
RouterA(config-router)#version 2
RouterA(config-router)#no auto
RouterA(config-router)#network 192.168.1.0
RouterA(config-router)#default information-ori
RouterA(config)#ip route 0.0.0.0 0.0.0.0 s1/0
SwitchA(config)#ip routing
SwitchA(config)#router rip
SwitchA(config-router)#version 2
SwitchA(config-router)#no auto
SwitchA(config-router)#network 192.168.1.0
SwitchA(config-router)#network 192.168.2.0
SwitchA(config-router)#network 192.168.10.0
SwitchA(config-router)#network 192.168.20.0
```

RouterB和RouterC是Internet路由器，配置OSPF协议。

内网配置RIP协议，Internet网络配置OSPF协议，出口路由器连接内网的接口配置RIP协议，连接Internet的接口配置默认路由指向外网，并将默认路由注入内网RIP协议中。

然后，在出口路由器上配置基于端口的NAT转换，让内网用户可以出去访问Internet。配置静态NAT转换，给Web服务器设置一对一的地址映射，提供对外网用户的访问服务。具体配置如以下代码所示：

```
RouterA(config)#access-list 1 permit 192.168.0.0 0.0.255.255
RouterA(config)#ip nat pool aaa 201.1.1.3 201.1.1.10 netmask 255.255.255.0
RouterA(config)#ip nat inside source list 1 pool aaa overload
RouterA(config)#ip nat inside source static 192.168.2.1 201.1.1.11
```

4.3.2 配置时间访问控制列表规则

在核心交换机上配置时间访问控制列表的规则。因为Web服务器和核心交换机相连，启用核心交换机的包过滤防火墙功能，定义好两个时间访问控制列表规则，一个规则定义内网用户访问服务的时间是周一到周日的8:00到20:00，另外一个规则定义Internet用户访问服务的时间是周一到周五的9:00到18:00。具体配置如以下代码所示：

```
SwitchA(config)#time-range aaa 8:00 to 20:00 Daily
SwitchA(config)#time-range bbb 9:00 to 18:00 Working-day
```

4.3.3 定义扩展访问控制列表并应用时间访问控制列表

在核心交换机上配置扩展访问控制列表，并将上面定义的时间访问控制列表应用到相应的扩展列表，具体配置如以下代码所示：

```
SwitchA(config)#access-list 100 permit tcp 192.168.10.0
                0.0.0.255 host 192.168.2.1 eq www time-range aaa
SwitchA(config)#access-list 100 permit tcp any host
                192.168.2.1 eq www time-range bbb
```

核心交换机的系统时间也要和当前的时间相对应，在核心交换机的特权模式下使用show clock命令先查看一下交换机的系统时间，如果不对，需要使用clock set命令重新进行设置，如以下代码所示：

```
SwitchA#show clock
0:4:25.359 UTC Mon Mar 1 1993
SwitchA#show clock
10:24:35.897 UTC Sun Feb 28 2021
```

由以上代码可以看到，第一次使用show clock命令查看核心交换机的系统时间是1993年，后来通过设置，再查询交换机的系统时间就和当前时间一致了。

4.3.4 将扩展列表绑定到端口

因为Web服务器和核心交换机相连，所以保护Web服务器的职责交给核心交换机，将扩展访问控制列表绑定到核心交换机的相应端口，数据包通过该接口的时候就进行访问控制列表规则检查[9]。对Web服务器访问的需求是，Web服务器对内网用户提供访问服务的时间是周一到周日的8:00到20:00，对Internet用户提供访问服务的时间是周一到周五的9:00到18:00，其他时间为服务器的数据备份时间。所以列表100绑定在核心交换机的F0/1，列表101绑定在核心交换机的F0/2，绑定方向都是in，如以下代码所示：

```
SwitchA(config)#int f0/1
SwitchA(config-if)#ip access-group 100 in
SwitchA(config)#int f0/2
SwitchA(config-if)#ip access-group 101 in
```

4.3.5 系统测试结果

最后，测试Web服务器被客户端访问情况，查看内网用户是否在规定的时间可以访问服务器，非规定时间不能访问服务器；查看Internet用户是否在规定的时间可以访问服务器，非规定时间不能访问服务器，如图2所示。

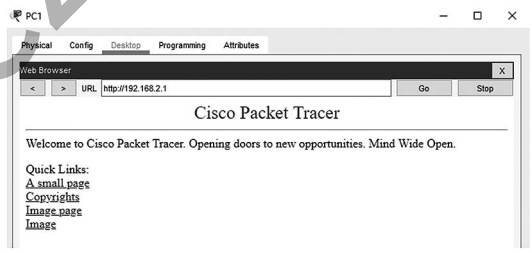

图2 PC1可以访问Web服务器

Fig.2 PC1 can access the web server

设定当前时间为周日10:42:20，查看内网用户和Internet用户分别访问Web服务器得到的响应情况。

查看Internet用户PC0访问情况，PC0根据Web服务器对外映射地址201.1.1.11访问，如图3所示。

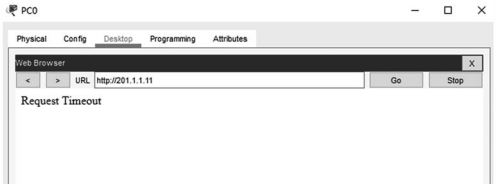

图3 PC0不可以访问Web服务器

Fig.3 PC0 cannot access the web server

5 结论(Conclusion)

本文主要论述了时间访问控制列表的定义规则和应用方法，并设定了一个系统实现不同用户对Web服务器访问的时间规定。系统集成了核心交换机包过滤防火墙技术、时间访问控制列表技术、扩展访问控制列表技术。最后，系统成功

(下转第62页)