CCNA中文笔记-ManagingTrafficwithAccessLists PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/143/2021_2022_CCNA_E4_B8_AD_E6_96_87_c102_143370.htm chapter9 managing traffic with access lists introduction to access lists 访问列表(access list,acl)的主要作用是过滤你不想要的数据包.设置acl的一些规则: 1.按顺序的比较,先比较第一行,再比较第二行..直到最后1行 2.从第一行起,直到找到1个符合条件的行.符合以后,其余的行就不再继续比较下去 3.默认在每个acl中最后1行为隐含的拒绝(deny),如果之前没找到1条许可(permit)语句,意味着包将被丢弃.所以每个acl必须至少要有1行permit语句,除非你想想所有数据包丢弃 2种主要的访问列表: 1.标准访问列表(standard access lists):只使用源ip地址来做过滤决定 2.扩展访问列表(extended access lists):它比较源ip地址和目标ip地址,层3的协议字段,层4端口号来做过滤决定 利用acl来过滤,必须把acl应用到需要过滤的那个router的接口上,否则acl是不会起到过滤作用的.而且你还要定义过滤的方向,比如是是想过滤从internet到你企业网的数据包呢还是想过滤从企业网传出到internet的数据包呢?方向分为下面2种: 1.inbound acl:先处理,再路由 2.outbound acl:先路由,再处理 一些设置acl的要点: 1.每个接口,每个方向,每种协议,你只能设置1个acl 2.组织好你的acl的顺序,比如测试性的最好放在acl的最顶部 3.你不可能从acl从除去1行,除去1行意味你将除去整个acl,命名访问列表(named access lists)例外(稍后介绍命名访问列表) 4.默认acl结尾语句是deny any,所以你要记住的是在acl里至少要有1条permit语句 5.记得创建了acl后要把它应用在需要过滤的接口上 6.acl是用于过滤经过router的数据包,它并

不会过滤router本身所产生的数据包 7.尽可能的把ip标准acl放置在离目标地址近的地方.尽可能的把ip扩展acl放置在离源地址近的地方 standard access lists 介绍acl设置之前先介绍下通配符掩码(wildcard masking).它是由0和255的4个8位位组组成的.0代表必须精确匹配,255代表随意,比如:172.16.30.0 0.0.0.255,这个告诉router前3位的8位位组必须精确匹配,后1位8位位组的值可以为任意值.如果你想指定172.16.8.0到172.16.15.0,则通配符掩码为0.0.7.255(15-8=7) 配置ip标准acl,在特权模式下使用access-lists [范围数字] [permit/deny] [any/host]命令.范围数字为1到99和1300到1999.permit/deny分别为允许和拒绝.any为任何主机,host为具体某个主机(需要跟上ip地址)或某1段 我们来看1个设置ip标准acl的实例: router有3个lan的连接1个internet的连接.现在,销售部的用户不允许访问金融部的用户,但是允许他们访问市场部和internet连接.配置如下:
router(config)#access-list 10 deny 172.16.40.0 0.0.0.255
router(config)#access-list 10 permit any 注意隐含的deny any,所以末尾这里我们要加上permit any,any等同于0.0.0.0 255.255.255.255.接下来把acl应用在接口上,之前说过了尽可能的把ip标准acl放置在离目标地址近的地方,所以使用ip access-group命令把acl 10放在e1接口,方向为出,即out.如下:
router(config)#int e1 router(config-if)#ip access-group 10 out
controlling vty(telnet) access 使用ip标准acl来控制vty线路的访问.配置步骤如下: 1.创建个ip标准acl来允许某些主机可以telnet 2.使用access-class命令来应用acl到vty线路上 实例如下:
router(config)#access-list 50 permit 172.16.10.3 router(config)#line vty 0 4 router(config-line)#access-class 50 in 如上,进入vty线路模

式,应用acl,方向为进来,即in.因为默认隐含的deny any,所以上面的例子,只允许ip地址为172.16.10.3的主机telnet到router上 extended access lists 扩展acl:命令是access-list [acl号] [permit/deny] [协议] [源地址] [目标地址] [操作符] [端口] [log].acl号的范围是100到199和2000到2699.协议为tcp,udp等,操作符号有eq(表等于),gt(大于),lt(小于)和neq(非等于)等等.log为可选,表示符合这个acl,就记录下这些日志 来看1个配置扩展acl的实例: http://bbs.**********.com/uploadfil...12392068957.jpg 假如要拒telnet和ftp到绝位于金融部的主机172.16.30.5,配置如下: