**思科ACL详解**

**基本原则**：1、按顺序执行，只要有一条满足，则不会继续查找

               2、隐含拒绝，如果都不匹配，那么一定匹配最后的隐含拒绝条目，思科默认的

              3、任何条件下只给用户能满足他们需求的最小权限

               4、不要忘记把ACL应用到端口上

**一、标准ACL**

命令：access-list {1-99} {permit/deny} source-ip source-wildcard [log]

    例：access-list 1 penmit 192.168.2.0 0.0.0.255      允许192.168.2.0网段的访问

      access-list 1 deny 192.168.1.0 0.0.0.255         拒绝192.168.1.0网段的访问

说明：wildcard为反掩码，host表示特定主机等同于192.168.2.3 0.0.0.0；any表示所有的源或目标等同于0.0.0.0 255.255.255.255；log表示有匹配时生成日志信息；标准ACL一般用在离目的最近的地方。

**二、扩展ACL**

命令：access-list {100-199} {permit/deny}  protocol source-ip source-wildcard  [operator port] destination-ip destination-wildcard  [operator port] [established][log]

例：access-list 101 permit tcp 192.168.2.0 0.0.0.255 gt 1023 host 192.168.1.2 eq 80

    允许192.168.2.0网段的主机访问主机192.168.1.2的web服务

      access-list 101 permit udp 192.168.2.0 0.0.0.255 gt 1023 any eq 53

     允许192.168.2.0网段的主机访问外网以做dns查询

  说明：gt 1023表示所有大于1023的端口，这是因为一般访问web、ftp等服务器时客户端的主机是使用一个1023以上的随机端口；established 表示允许一个已经建立的连接的流量，也就是数据包的ACK位已设置的包。

**三、命名ACL**

命令： ip access-list {standard/extended} name

 { permit /deny} source-ip source-wildcard        标准

        { permit /deny} protocol source-ip source-wildcard [operator port] destination-ip destination-wildcard  [operator port] [established][log]     扩展

例：ip access-list extended outbound       定义一个名为outbound的命名ACL

  permit tcp 192.168.2.0 0.0.0.255 gt 1023 host 192.168.1.2 eq 80

    允许192.168.2.0网段的主机访问主机192.168.1.2的web服务

**四、动态ACL**

   动态ACL是一种利用路由器telnet的验证机制，动态建立临时的ACL以让用户可以暂时访问内网的一种技术

   命令：access-list {100-199} dynamic username [timeout minutes] permit any dest-ip dest-wildcard

  说明：username 必须是路由器上的某一个用户；timeout为绝对超时时间；最好定义dest-ip为外网要访问的服务器的IP.

例： 1：username lyl password lyl               建立用户，用于用户验证  
            2：access-list 101 permit tcp any host 10.10.1.1  eq 23   允许外网用户访问 路由器外端口的telnet服务，用于验证

access-list 101 permit tcp any host 10.10.1.1  eq 3001   允许外网用户访问路由器外端口的3001端口，用于telnet管理

 access-list 101 dynamic lyl timeout 8 permit ip any host 192.168.2.3 引用路由器上的lyl用户以建立动态的ACL

3、line vty 0 3

login local                   定义本地验证

  autocommand access-enable host timeout 3          用于动态ACL验证用户，此处host绝不可少，如果没有则生成的动态ACL源地址将为 any,则动态ACL毫无意义

      line vty 4

login local

rotary  1                         用开telnet管理，端口为3001

4、int s1/0

ip add 10.10.1.1 255.255.255.252

no shut

 ip access-group 101 in

**五、自反ACL**

基本思想：内网可以访问外网，但外网没有允许不能访问内网，内网访问外网的回应数据可以通过

例：一、ip access-list extended outbound         创建出去数据的ACL

      permit tcp any any reflect cisco    tcp的流量可以进来，但要在有内部tcp流量出去时动态创建

     二、 ip access-list extended inbound       创建进来数据的ACL

permit icmp any any          允许基于ICMP的数据如echo-request

                       evaluate cisco                   允许出去的ACL中的有cisco对应语句的TCP流量进来

     三、 int s1/0     s1/0为路由器的接外网的端口

ip access-group outbound out

 ip access-group inbound in

说明：reflect和evalute后面的对应名应该相同，此例中为cisco