运用ACL来构建坚固的防火墙体系 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/181/2021_2022__E8_BF_90_E7_94_A8ACL_E6_c101_181893.htm 网络防火墙安全策略是指要明确定义哪些数据包允许或禁止通过并使用网络服务，以及这些服务的使用规则。而且，网络防火墙安全策略中的每一条规定都应该在实际应用时得到实现。下面我们就路由器下通过访问控制列表实现安全策略，以达到防火墙的功能，并对其实现及应用进行详细的叙述。 访问控制列表的作用 访问控制列表是应用在路由器接口的指令列表，这些指令列表用来告诉路由器哪些数据包可以接收、哪些数据包需要拒绝。至于数据包是被接收还是被拒绝，可以由类似于源地址、目的地址、端口号、协议等特定指示条件来决定。通过灵活地增加访问控制列表，ACL可以当作一种网络控制的有力工具，用来过滤流入和流出路由器接口的数据包。 建立访问控制列表后，可以限制网络流量，提高网络性能，对通信流量起到控制的手段，这也是对网络访问的基本安全手段。在路由器的接口上配置访问控制列表后，可以对入站接口、出站接口及通过路由器中继的数据包进行安全检测。 IP访问控制列表的分类 标准IP访问控制列表 当我们要想阻止来自某一网络的所有通信流量，或者充许来自某一特定网络的所有通信流量，或者想要拒绝某一协议簇的所有通信流量时，可以使用标准访问控制列表来实现这一目标。标准访问控制列表检查路由的数据包的源地址，从而允许或拒绝基于网络、子网或主机的IP地址的所有通信流量通过路由器的出口。 扩展IP访问控制列表 扩展访问控制列表既检查数据包的源地址，也

检查数据包的目的地址，还检查数据包的特定协议类型、端口号等。扩展访问控制列表更具有灵活性和可扩充性，即可以对同一地址允许使用某些协议通信流量通过，而拒绝使用其他协议的流量通过。 命名访问控制列表 在标准与扩展访问控制列表中均要使用表号，而在命名访问控制列表中使用一个字母或数字组合的字符串来代替前面所使用的数字。使用命名访问控制列表可以用来删除某一条特定的控制条目，这样可以让我们在使用过程中方便地进行修改。 在使用命名访问控制列表时，要求路由器的IOS在11.2以上的版本，并且不能以同一名字命名多个ACL，不同类型的ACL也不能使用相同的名字。 通配符掩码 通配符掩码是一个32比特位的数字字符串，它被用点号分成4个8位组，每组包含8比特位。在通配符掩码位中，0表示“ 检查相应的位 ”，1表示“ 不检查相应的位 ”。通配符掩码与IP地址是成对出现的，通配符掩码与子网掩码工作原理是不同的。在IP子网掩码中，数字1和0用来决定是网络、子网，还是相应的主机的IP地址。如表示172.16.0.0这个网段，使用通配符掩码应为0.0.255.255。 在通配符掩码中，可以用255.255.255.255表示所有IP地址，因为全为1说明所有32位都不检查相应的位，这是可以用any来取代。而0.0.0.0的通配符掩码则表示所有32位都要进行匹配，这样只表示一个IP地址，可以用host表示。所以在访问控制列表中，可以选择其中一种表示方法来说明网络、子网或主机。 实现方法 首先在全局配置模式下定义访问列表，然后将其应用到接口中，使通过该接口的数据包需要进行相应的匹配，然后决定被通过还是拒绝。并且访问列表语句按顺序、逻辑地处理，它们在列表中自上向下开始匹配数据包。如果一个数

据包头与访问权限表的某一语句不匹配，则继续检测列表中的下一个语句。在执行到访问列表的最后，还没有与其相匹配的语句，数据包将被隐含的“ 拒绝 ”语句所拒绝。 标准IP访问控制列表 在实现过程中应给每一条访问控制列表加上相应的编号。标准IP访问控制列表的编号为1至99，作用是阻止某一网络的所有通信流量，或允许某一网络的所有通信流量。语法为： Router(config)#access-list access-list-number(1~99) {deny|permit} source [source-wildcard] 如果没有写通配符掩码，则默认值会根据源地址自动进行匹配。下面举例来说明：要阻止源主机为 192.168.0.45的一台主机通过E0，而允许其他的通讯流量通过E0端口。 Router(config)#access-list 1 deny 192.168.0.45 0.0.0.0 或Router(config)#access-list 1 deny host 192.168.0.45 或Router(config)#access-list 1 deny 192.168.0.45 Router(config)#access-list 1 permit any Router(config)#interface ethernet 0 Router(config-if)#ip access-group 1 in 首先我们在全局配置模式下定义一条拒绝192.168.0.45主机通过的语句，通配符掩码可以使用0.0.0.0或host，或使用缺省值来表示一台主机，然后将其访问列表应用到接口中。如果现在又修改了计算机的IP地址，那么这条访问控制列表将对您不起作用。 扩展IP访问控制列表 扩展IP访问控制列表的编号为100至199，并且功能更加灵活。例如，要阻止192.168.0.45主机Telnet流量，而允许Ping流量。 Router(config)#access-list 101 permit icmp 192.168.0.45 0.0.0.0 any Router(config)#access-list 101 deny tcp 192.168.0.45 0.0.0.0 any eq 23 Router(config)#access-list 101 permit ip any any Router(config)#interface ethernet 0 Router(config-if)#ip access-group 101 in 因为Ping命令使用网络层的ICMP协议，所

以让ICMP协议通过。而Telnet使用端口23，所以将端口号为23的数据包拒绝了，最终应用到某一接口，这样就可以达到目的。 命名访问控制列表 对于某一给定的协议，在同一路由器上有超过99条的标准ACL，或有超过100条的扩展ACL。想要通过一个字母数字串组成的名字来直观地表示特定的ACL时，并且路由器的IOS版本在11.2及以上时，可以使用命名访问控制列表，也就是用某些字符串来取代标准与扩展ACL的访问列表号。命名访问控制列表的语法格式为：Router(config)#ip access-list {standard|extended} name 在ACL配置模式下，通过指定一个或多个允许或拒绝条件，来决定一个数据包是允许通过还是被丢弃。语法格式如下：Router(config{std-|ext-}nacl)#{permit|deny} {source [source-wildcad]|any} 下面是一个配置实例： ip access-list extended nyist permit tcp 172.16.0.0 0.0.255.255 any eq 23 deny tcp any any deny udp 172.16.0.0 0.0.255.255 any lt 1024 interface Ethernet 0 ip access-group nyist in 基于时间访问列表的应用 随着网络的发展和用户要求的变化，从IOS 12.0开始，思科(CISCO)路由器新增加了一种基于时间的访问列表。通过它，可以根据一天中的不同时间，或者根据一星期中的不同日期，或二者相结合来控制网络数据包的转发。这种基于时间的访问列表，就是在原来的标准访问列表和扩展访问列表中，加入有效的时间范围来更合理有效地控制网络。首先定义一个时间范围，然后在原来的各种访问列表的基础上应用它。 基于时间访问列表的设计中，用time-range 命令来指定时间范围的名称，然后用absolute命令，或者一个或多个periodic命令来具体定义时间范围。IOS命令格式为：

time-range time-range-name absolute [start time date] [end time date] periodic days-of-the week hh:mm to [days-of-the week] hh:mm 下面分别来介绍一下每个命令和参数的详细情况： time-range 用来定义时间范围的命令。 time-range-name 时间范围名称，用来标识时间范围，以便于在后面的访问列表中引用。 absolute 该命令用来指定绝对时间范围。它后面紧跟着start和end两个关键字。在这两个关键字后面的时间要以24小时制hh:mm表示，日期要按照日/月/年来表示。如果省略start及其后面的时间，则表示与之相联系的permit 或deny语句立即生效，并一直作用到end处的时间为止。如果省略end及其后面的时间，则表示与之相联系的permit 或deny语句在start处表示的时间开始生效，并且一直进行下去。 periodic 主要是以星期为参数来定义时间范围的一个命令。它的参数主要有Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、Sunday中的一个或者几个的组合，也可以是daily(每天)、weekday(周一至周五)，或者weekend(周末)。 下面我们来看一个实例：在一个网络中，路由器的以太网接口E0连接着202.102.240.0网络，还有一个串口S0连入Internet。为了让202.102.240.0网络内的公司员工在工作时间内不能进行WEB浏览，从2003年5月1日1时到2003年5月31日晚24时这一个月中，只有在周六早7时到周日晚10时才可以通过公司的网络访问Internet。 我们通过基于时间的扩展访问控制列表来实现这一功能： Router# config t Router(config)# interface Ethernet 0 Router(config-if)#ip access-group 101 in Router(config-if)#time-range http Router(config-if)#absolute start 1:00 1 may 2003 end 24:00 31 may 2003 periodic Saturday 7:00 to

Sunday 22:00 Router(config-if)#ip access-list 101 permit tcp any any eq 80 http 我们是在一个扩展访问列表的基础上，再加上时间控制就达到了目的。因为是控制WEB访问的协议，所以必须要用扩展列表，那么编号需在100至199之间。我们定义了这个时间范围的名称是http，这样，我们就在列表中的最后一句方便地引用了。 合理有效地利用基于时间的访问控制列表，可以更有效、更安全、更方便地保护我们的内部网络，这样您的网络才会更安全，网络管理人员也会更加轻松。 检验 在路由器中用show running-config命令检查当前正在运行的配置文件，用show ip access-list命令来查看访问控制列表，并在计算机的命令提示符下用Ping/Telnet命令进行测试。 总结 在网络安全体系中，最重要的安全要素访问控制的控制点在网络通信通道的出入口上。内部网络通过路由器的广域网接口与Internet相连，再通过此路由器的局域网接口接入内部网络，而正确地放置ACL访问控制列表将起到防火墙的作用。为了满足与Internet间的访问控制，以及满足内部网络不同安全属性网络间的访问控制要求，在路由器上配置防火墙，让网络通信均通过它，以此控制网络通信及网络应用的访问权限。