一个动态ACL的案例 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/284/2021_2022__E4_B8_80_E4_B8_AA_E5_8A_A8_E6_c101_284828.htm 所在的单位有一台路由器将两个以太网段连到了internet上，路由器是通过串行端口0连 到internet上的，而以太网分别通过端口E 0和E 1连到路由器上。假设我们希望允许任 何用户都能通过I P访问1 9 8 . 7 8 . 4 6 . 1 2服务器，并允许2 0 5 . 1 3 1 . 1 7 5 . 0网络上的用户通过We b浏览（h t t p）和F T P访问I n t e r n e t。 useranme test password cisco ! int serial 0 ip add 175.10.1.1 255.255.255.0 ip access-group 100 in ! access-list 100 permit tcp any host 175.10.1.1 eq telnet access-list 100 permit udp any eq 53 205.131.175.0 0.0.0.255 gt 1023 established access-list 100 permit tcp any eq 21 205.131.175.0 0.0.0.255 gt 1023 established access-list 100 permit tcp any eq 20 205.131.175.0 0.0.0.255 gt 1023 access-list 100 dynamic test timeout 180 permit ip any host 198.76.46.12 log ! logging buffered 64000 ! line vty 0 2 login local autocommand access-enable host timeout 10 line vty 3 4 login local rotary 1 首先，我们注意到访问表被应用到了串行端口上。将扩展访问表应用到离过滤源最近的 地方，这是一种很好的方法。在本例中，我们的目的是要过滤I n t e r n e t上的主机，所以串行端口是路由器上离被过滤主机最近的端口。访问表应用的方向是向内的，因 为从路由器的角度看来， I n t e r n e t来的报文是流向路由器的。如果我们将访问 表应用成向外的访问，则过滤的报文将是离开串行接口而通往I n t e r n e t的报文， 而这并非我们所希望的。另外，我们还建立了一个用户名“ t e s t”，它可以用来访问路由器

。在实际应用中，我们应该为每个用户建立一对用 户名和口令。现在，让我们再分析访问表的每一个表项。 第一个表项允许从任何源IP地址来的报文到达主机175.10.1.1，如果其目标 端口为telnet（23）的话。这样，我们实际上允许了向内的telnet连接到路 由器的串行接口。我们可以允许向内的telnet，连接到路由器的其他IP地址，但 只允许向内访问路由器的串行接口是一种最佳的选择。 第二个表项允许从任何源IP地址来的报文，如果其源端口是域名系统（domain namesystem, DNS）（UDP 53），且目标网络位于205.131.175.0/24， 目的端口大于1023的话。这将允许DNS应答到达205.131.175.0/24网络。所有有效DNS请求的源端口应该为1024或更大，因此有效DNS的应答就应 发送到此1024或更高的端口。如果我们不指定目的端口大于1023，则攻击者可以 从源端口53发送UDP报文到达我们的网络，从而导致对内部服务器的拒绝服务（denial-of-service, DOS）攻击。大量的服务器端口都处于小于1024的保留区间内，所以我们应阻塞目的端口小于1024的报文，以关闭潜在的安全漏洞。 第三和第四个表项允许具有如下特征的报文进入：源端口为WWW（TCP 80）或FTP（TCP 21），目标位于205.131.175.0/24网络，目标端口大于1023， 且TCP头中设置了ACK和RST位。这两个表项允许由内部主机发起的WWW和FTP会 话的返回报文。指定源端口和目的端口的原因与第二个表项相同。使用established意味着只有设置了应答位（ACK）和复位位（RST）的报文才能够匹配并允许通过访问表项。只有那些已经建立了TCP会话的报文才会设置这些位，这样增加了访 问表的安全层次。值得注意的是，

攻击者很容易在向内的报文中手工设置这些位，所以这种检测是十分简单的。但是，如果内部网络采用正确的TCP/IP协议栈，它们就会忽略这些带ACK和RST位的向内报文，因为它们不是主机上合法的TCP会话的一部分，这就是为什么established关键字仍然十分重要的原因。注意，这种检验对UDP报文是无用的，这就是为什么在第二个访问表项中没有该关键字的原因。第五个表项允许那些从源端口为20的任何主机向内报文到达网络205.131.175.0/24的主机，如果其目的端口大于1023的话，允许了那些由内部主机发起的FTP部分数据的报文连接到内部主机。FTP协议实现的标准实现需要FTP服务器发回一个到源FTP客户机连接。该连接的初始报文没有设置ACK或RST位，所以我们在表项中不能使用established关键字。有一种版本的FTP称为被动模式（passive mode）的FTP，或称为PASC，它不需要服务器发起一个向源FTP客户机的连接。在这种模式的FTP中，客户机需要发起到FTP服务器非20端口的另一个连接。该端口是大于1023的一种随机选择。我们允许所有大于1023 TCP端口的报文通过，是因为我们不能进一步确定FTP服务器会选择哪一个端口（被动模式FTP服务器的数据端口不为20，这与普通模式FTP是不同的）。尽管我们不能让该表项如我们所希望的那样确切，established关键字仍能使该表项比允许外部发起向内部网络的会话要安全一些。第六个表项（也是最后一个表项）为动态访问表项，它允许来自被认证主机的报文到达服务器198.78.46.12。我们定义的绝对超时时间为3小时（180分钟），并对该表项进行了日志记录（我们还开启了路由器缓冲区的日志）。通过将匹配动态表项的报

文进行记录，我们可以跟踪用户的行为，并建立一个普通的基线。这样，我们可以发现不正常的行为，并由此判断这是否是由攻击者产生的。我们还将动态访问表项的空闲时间设置成了10分钟，这是在vty线配置中通过autocommand设置的。最好是将这两个值都设上，这样我们能减少动态表项处于活跃状态的时间，因此也减少了攻击者冲破动态表项的可能性。 空闲计时器在每有一个报文匹配动态访问表项时进行复位。而绝对计时器是不复位的。即使一个会话仍然处于活跃状态，如果绝对超时达到，动态表项就会被删除，从而用户需要再经过一个认证过程。如果他们有经过路由器的活跃会话，这些会话将被终止。正因如此，我们建议将绝对超时设置得相对大一些，一般为一个小时或更长一些的时间。但我们应该将空闲时间设置得小一些，一般为10分钟或更短的时间。我们认为，不应将空闲时间的设置大于30钟。