如何监视和测试访问控制列表配置 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/271/2021_2022__E5_A6_82_E4_BD_95_E7_9B_91_E8_c101_271547.htm 我们让R2作为内部网络，R3作为内部网络，以下配置使R2发起访问R3没问题，从R3访问R2则被拒绝。注意这个配置方案是针对基于TCP的应用，任何 TCP通讯都是双向的，从R2发起的访问外部网络之后，外部网络的流量得以通过，这个时候TCP报文，ACK或RST位被设置为1R1(configure)access-list 101 permit tcp any any established log-inputR1(configure)access-list 101 permit ospf any anyR1(configure)access-list 101 deny ip any any log-inputR1(configure)int s2/1R1(configure-if)ip access-group 101 in 以上log-input是为了显示监视数据报文被过滤的情况，接下来用debug ip packet detailed来监视报文经过R1的情况，应该路由器还有OSPF报文产生，因此我们对DEBUG信息做了限制。r1(config)#access-list 102 permit tcp any any 我们这样做 让R2发起telnet访问R3r1#telnet 3.3.3.3Trying 3.3.3.3 ... Openr3>*Mar 1 00:55:53.003: IP: tableid=0, s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), routed via RIB*Mar 1 00:55:53.003: IP: s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), len 44, sending*Mar 1 00:55:53.007: TCP src=11001, dst=23, seq=2398697781, ack=0, win=4128 SYN*Mar 1 00:55:53.179: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 3.3.3.3(23) (Serial2/1 ) -> 13.1.1.1(11001), 1 packet*Mar 1 00:55:53.183: IP: tableid=0, s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), routed via RIB*Mar 1 00:55:53.183: IP: s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), len 44, rcvd 3*Mar 1

00:55:53.187: TCP src=23, dst=11001, seq=949632690, ack=2398697782, win=4128 ACK SYN*Mar 1 00:55:53.187: IP: tableid=0, s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), routed via RIB*Mar 1 00:55:53.191: IP: s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), len 40, sending*Mar 1 00:55:53.191: TCP src=11001, dst=23, seq=2398697782, ack=949632691, win=4128 ACK*Mar 1 00:55:53.199: IP: tableid=0, s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), routed via RIB*Mar 1 00:55:53.203: IP: s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), len 49, sending*Mar 1 00:55:53.203: TCP src=11001, dst=23, seq=2398697782, ack=949632691, win=4128 ACK PSH*Mar 1 00:55:53.207: IP: tableid=0, s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), routed via RIB*Mar 1 00:55:53.211: IP: s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), len 40, sending*Mar 1 00:55:53.215: TCP src=11001, dst=23, seq=2398697791, ack=949632691, win=4128 ACK*Mar 1 00:55:53.455: IP: tableid=0, s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), routed via RIB*Mar 1 00:55:53.455: IP: s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), len 52, rcvd 3*Mar 1 00:55:53.459: TCP src=23, dst=11001, seq=949632691, ack=2398697791, win=4119 ACK PSH*Mar 1 00:55:53.459: IP: tableid=0, s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), routed via RIB*Mar 1 00:55:53.463: IP: s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), len 45, rcvd 3*Mar 1 00:55:53.467: TCP src=23, dst=11001, seq=949632703, ack=2398697791, win=4119 ACK PSH*Mar 1 00:55:53.467: IP: tableid=0, s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), routed via RIB*Mar 1 00:55:53.471: IP: s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), len 43, rcvd 3*Mar 1

00:55:53.471: TCP src=23, dst=11001, seq=949632708, ack=2398697791, win=4119 ACK PSH*Mar 1 00:55:53.475: IP: tableid=0, s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), routed via RIB*Mar 1 00:55:53.479: IP: s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), len 46, rcvd 3*Mar 1 00:55:53.479: TCP src=23, dst=11001, seq=949632711, ack=2398697791, win=4119 ACK PSH*Mar 1 00:55:53.483: IP: tableid=0, s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), routed via RIB*Mar 1 00:55:53.487: IP: s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), len 43, sending*Mar 1 00:55:53.487: TCP src=11001, dst=23, seq=2398697791, ack=949632717, win=4102 ACK PSH*Mar 1 00:55:53.491: IP: tableid=0, s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), routed via RIB*Mar 1 00:55:53.495: IP: s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), len 43, sending*Mar 1 00:55:53.495: TCP src=11001, dst=23, seq=2398697794, ack=949632717, win=4102 ACK PSH*Mar 1 00:55:53.499: IP: tableid=0, s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), routed via RIB*Mar 1 00:55:53.503: IP: s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), len 49, sending*Mar 1 00:55:53.503: TCP src=11001, dst=23, seq=2398697797, ack=949632717, win=4102 ACK PSH*Mar 1 00:55:53.659: IP: tableid=0, s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), routed via RIB*Mar 1 00:55:53.663: IP: s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), len 43, rcvd 3*Mar 1 00:55:53.663: TCP src=23, dst=11001, seq=949632717, ack=2398697797, win=4113 ACK PSH*Mar 1 00:55:53.867: IP: tableid=0, s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1), routed via RIB*Mar 1 00:55:53.867: IP: s=13.1.1.1 (local), d=3.3.3.3 (Serial2/1),

len 40, sending*Mar 1 00:55:53.871: TCP src=11001, dst=23, seq=2398697806, ack=949632720, win=4099 ACK*Mar 1 00:55:53.963: IP: tableid=0, s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), routed via RIB*Mar 1 00:55:53.967: IP: s=3.3.3.3 (Serial2/1), d=13.1.1.1 (Serial2/1), len 40, rcvd 3*Mar 1 00:55:53.967: TCP src=23, dst=11001, seq=949632720, ack=2398697806, win=4104 ACK 注意R3返回R2的数据报文得以通过，接下来我们测试从R3发起访问R2的情况r3#telnet 2.2.2.2Trying 2.2.2.2 ...% Destination unreachable. gateway or host downr1#*Mar 1 01:02:22.779: %SEC-6-IPACCESSLOGP: list 101 denied tcp 13.1.1.3(11002) (Serial2/1 ) -> 2.2.2.2(23), 1 packet*Mar 1 01:02:22.783: IP: s=13.1.1.3 (Serial2/1), d=2.2.2.2, len 44, access denied*Mar 1 01:02:22.783: IP: tableid=0, s=13.1.1.1 (local), d=13.1.1.3 (Serial2/1), routed via RIB*Mar 1 01:02:22.787: IP: s=13.1.1.1 (local), d=13.1.1.3 (Serial2/1), len 56, sending*Mar 1 01:02:24.139: IP: s=12.1.1.2 (Serial2/0), d=224.0.0.5, len 80, rcvd 0*Mar 1 01:02:24.315: IP: s=13.1.1.1 (local), d=224.0.0.5 (Serial2/1), len 80, sending broad/multicast*Mar 1 01:02:25.139: IP: s=12.1.1.1 (local), d=224.0.0.5 (Serial2/0), len 80, sending broad/multicast 注意，TCP协议的第一次发送是SYN字段，这是用来同步准备建立一个新连接的两端主机，而ACK位由接收者置位从而向发送者表明数据已经成功接收。 RST（reset）位说明什么时候重新启动连接。带Eetablished的扩展访问列表只允许ACK或RST位置1的TCP报文通过。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com