路由器设置莫让ACL的设置形同虚设 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E8_B7_AF_E7_94_B1_E5_99_A8_E8_c101_461747.htm 大家都知道通过在路由器或交换机上设置访问控制列表ACL，可以在一定程度上起到提高安全，防范黑客与病毒攻击的效果，笔者所在公司也一直在使用这个方法。 然而，笔者却在实际工作中发现了一个影响安全的问题，如果对路由器的默认设置不注意的话，很可能会让强大的ACL列表失效，就好比二战的马其诺防线一样，病毒与黑客可以非常轻松地绕道攻击内网计算机。 安全分析： 有过路由器配置经验的读者应该知道网络管理员经常通过在路由器或交换机上设置访问控制列表来完成防范病毒和黑客的作用。Cisco出品的路由器或交换机的访问控制列表都默认在结尾添加了“ DENY ANY ANY ”语句，这句话的意思是将所有不符合访问控制列表（ACL）语句设定规则的数据包丢弃。 最近笔者所在公司添置了华为的2621系列路由器，一般情况下CISCO和华为设备的配置方法基本相同，所以笔者按照在Cisco路由器上的设置语句制定了ACL规则，并将这些规则输入到华为路由器上。由于CISCO默认自动添加DENY ANY ANY语句，所以笔者也想当然的认为华为路由器也会默认将这个命令添加。然而，在配置后却发现所有ACL过滤规则都没有生效，该过滤的数据包仍然被路由器正常转发。 经过反复研究、查询资料，笔者发现原来华为公司的访问控制列表在结尾处添加的是“ PERMIT ANY ANY ”语句，这样对于不符合访问控制列表（ACL）语句设定规则的数据包将容许通过，这样造成了一个严重后果，那就是不

符合ACL设定规则的数据包也将被路由器无条件转发而不是Cisco公司采用的丢弃处理，这造成了该过滤的数据包没有被过滤，网内安全岌岌可危。非法数据包绕过了网络管理员精心设置的防病毒“ 马其诺防线 ”，从而轻而易举的侵入了用户的内网。 解决措施： 如何解决这个问题呢？这个问题是因为华为路由器的默认设置造成的。我们可以在ACL的最后添加上“ DENY ANY ANY ”语句或将默认的ACL结尾语句设置为DENY ANY ANY.头一种方法仅仅对当前设置的ACL生效，以后设置新ACL时路由器还是默认容许所有数据包通过；而第二种方法则将修改路由器的默认值，将其修改成和CISCO设备一样的默认阻止所有数据包。 1、ACL规则直接添加法 在华为设备上设置完所有ACL语句后再使用“ rule deny ip source any destination any ”将没有符合规则的数据包实施丢弃处理。 2.修改默认设置法 在华为设备上使用“ firewall default deny ”，将默认设置从容许转发变为丢弃数据包。从而一劳百逸的解决默认漏洞问题。因此笔者推荐大家使用第二种方法解决这个默认设置的缺陷问题。 总结： 经过这次“ 马其诺 ”事件，我们可以发现即使是相同的配置命令，如果厂商不同最好事先查阅一下用户手册（特别注意默认设置），往往默认设置会造成很多不明不白的故障。发现问题以后也不要轻易怀疑设备硬件有问题，应该多从软件及配置命令入手查找问题所在。一个小小的默认设置就将精心打造的防病毒体系完全突破，所以对于我们这些网络管理员来说每次设置后都应该仔细测试下网络状况，确保所实施的手段得以生效。 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