AR系列路由器对网络病毒的应对办法

姚忆斌　2006-08-31 发表

AR系列路由器对网络病毒的应对办法

1、路由器的功能是保持网络的连通性，尽自己最大能力转发数据包。网络病毒发送的大
量垃圾报文，路由器是并不能识别的。
需要我们手工配置acl，比如最近流行的冲击波病毒，通过配置，路由器可以部分阻止这些垃圾报文。
禁止端口号为135的tcp报文
禁止端口号为69的udp报文
禁止icmp报文
以上只是辅助措施，**根本解决办法是查杀pc的病毒**，尽快安装微软操作系统的补丁，升级杀毒工具的病毒库，提高安全意识。

2、常见防病毒ACL，包含常见的病毒端口，新发现的病毒，还需要手工添加对应的端口
号，配置好以后在相关的端口下发即可。
病毒的攻击，可能来自公网，也可能来自内网。

```
acl number 3001
rule 0 deny tcp source-port eq 3127
rule 1 deny tcp source-port eq 1025
rule 2 deny tcp source-port eq 5554
rule 3 deny tcp source-port eq 9996
rule 4 deny tcp source-port eq 1068
rule 5 deny tcp source-port eq 135
rule 6 deny udp source-port eq 135
rule 7 deny tcp source-port eq 137
rule 8 deny udp source-port eq netbios-ns
rule 9 deny tcp source-port eq 138
rule 10 deny udp source-port eq netbios-dgm
rule 11 deny tcp source-port eq 139
rule 12 deny udp source-port eq netbios-ssn
rule 13 deny tcp source-port eq 593
rule 14 deny tcp source-port eq 4444
rule 15 deny tcp source-port eq 5800
rule 16 deny tcp source-port eq 5900
rule 18 deny tcp source-port eq 8998
rule 19 deny tcp source-port eq 445
rule 20 deny udp source-port eq 445
rule 21 deny udp source-port eq 1434
rule 30 deny tcp destination-port eq 3127
rule 31 deny tcp  destination-port eq 1025
rule 32 deny tcp destination-port eq 5554
rule 33 deny tcp destination-port eq 9996
rule 34 deny tcp destination-port eq 1068
rule 35 deny tcp destination-port eq 135
rule 36 deny udp destination-port eq 135
rule 37 deny tcp destination-port eq 137
rule 38 deny udp destination-port eq netbios-ns
rule 39 deny tcp destination-port eq 138
rule 40 deny udp destination-port eq netbios-dgm
rule 41 deny tcp destination-port eq 139
rule 42 deny udp destination-port eq netbios-ssn
rule 43 deny tcp destination-port eq 593
rule 44 deny tcp destination-port eq 4444
rule 45 deny tcp destination-port eq 5800
rule 46 deny tcp destination-port eq 5900
rule 48 deny tcp destination-port eq 8998
rule 49 deny tcp destination-port eq 445
```

```
rule 50 deny udp destination-port eq 445
rule 51 deny udp destination-port eq 1434
```