AR系列路由器包过滤控制访问列表的配置

姚忆斌　2006-08-31 发表

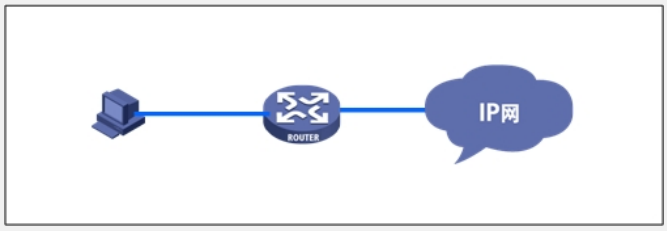
AR系列路由器包过滤控制访问列表的配置

【需求】

1、对内网地址192.168.1.0/25访问外网不作限制

2、对于内网地址192.168.1.128/25只允许收发邮件，不允许访问外网

【组网图】



【配置脚本】

配置脚本

```
#
sysname RouterA
#
firewall enable                          /使能防火墙功能/
firewall default deny                    /配置防火墙缺省操作为deny/
#
radius scheme system
#
domain system
#
acl number 2000                          /定义用于NAT转换的ACL/
rule 0 permit source 192.168.1.0 0.0.0.255
rule 1 deny
#
acl number 3001                          /定义用于包过滤的ACL/
rule 0 permit ip source 192.168.1.0 0.0.0.127
                                         /内网地址192.168.1.0/25访问外网不作限制/
rule 1 permit tcp source 192.168.1.128 0.0.0.127 destination-port eq pop3
rule 2 permit tcp source 192.168.1.128 0.0.0.127 destination-port eq smtp
                                         /内网地址192.168.1.128/25只能收发邮件/
#
interface Ethernet1/0/0
ip address 192.168.1.1 255.255.255.0
firewall packet-filter 3001 inbound      /对inbound流量使用包过滤/
#
interface Serial2/0/0
link-protocol ppp
ip address 202.101.1.2 255.255.255.252
nat outbound 2000
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 202.101.1.1 preference 60
#
user-interface con 0
user-interface vty 0 4
#
return
```

【验证】

通过查看disp firewall-statistics all、disp acl 3001确认防火墙确实生效

<RouterA>disp firewall-statistics all

Firewall is enable, default filtering method is 'deny'.
Interface: Ethernet1/0/0
In-bound Policy: acl 3001
Fragments matched normally
From 2006-05-31 5:05:50 to 2006-05-31 6:32:49
198 packets, 24129 bytes, 4% permitted,
0 packets, 0 bytes, 0% denied,
0 packets, 0 bytes, 0% permitted default,
5919 packets, 1021492 bytes, 96% denied default,
Totally 198 packets, 24129 bytes, 4% permitted,
Totally 5919 packets, 1021492 bytes, 96% denied.

<RouterA>disp acl 3001
Advanced ACL 3001, 3 rules
Acl's step is 1
rule 0 permit ip source 192.168.1.0 0.0.0.127 (194 times matched)
rule 1 permit tcp source 192.168.1.128 0.0.0.127 destination-port eq pop3 (9 times matched)
rule 2 permit tcp source 192.168.1.128 0.0.0.127 destination-port eq smtp (0 times matched)

【提示】

1、 系统缺省情况下为禁止防火墙（**firewall disable**），需要使用命令“**firewall enable**”来使能防火墙功能

2、 防火墙缺省过滤方式为允许通过（permit），可以通过“**firewall default deny**”修改为禁止通过

3、 在内网使用包过滤，并同时使用DHCP server分配地址时，需要在acl 3001中添加一条“**rule 0 permit ip source 0.0.0.0 0**”否则会出现DHCP Server无法分配地址的问题。