Typical Configuration of Packet Filtering ACL on AR Series Routers

姚忆斌 2007-09-13 发表

Typical Configuration of Packet Filtering ACL on AR Series Routers

[Requirements]

1. The intranet address 192.168.1.0/25 can freely access external networks.
2. The intranet address 192.168.1.128/25 can only send and receive e-mails rather than access to external networks.

[Networking diagram]

[Configuration script]

Configuration script

```
#
sysname RouterA
#
firewall enable                          /Enable firewall/
firewall default deny                      /Set default operation of firewall to deny/
#
radius scheme system
#
domain system
#
acl number 2000                            /Define an ACL for the NAT/
rule 0 permit source 192.168.1.0 0.0.0.255
rule 1 deny
#
acl number 3001                            /Define an ACL for packet filtering/
rule 0 permit ip source 192.168.1.0 0.0.0.127
                                        /Permit the intranet address
                    192.168.1.0/25 to freely access external networks/
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
                                        /Permit the intranet address
                    192.168.1.128/25 only to send and receive e-mails/
#
interface Ethernet1/0/0
ip address 192.168.1.1 255.255.255.0
firewall packet-filter 3001 inbound     /Apply packet filtering to the inbound flow/
#
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
```

[Verification]

Execute the **disp firewall-statistics all** and **disp acl 3001** commands to make sure that

the firewall does take effect.

```
<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)
```

[Tip]

1. By default, the firewall is disabled (firewall disable). You can execute the firewall enable command to enable it.
2. The default filtering mode of the firewall is permit. You can execute the firewall default deny command to change it.
3. Where packet filtering is applied on the intranet and the DHCP server is used to allocate addresses, you shall add rule 0 permit ip source 0.0.0.0 0 to acl 3001; otherwise, the DHCP server fails to allocate addresses.