Typical Reflexive ACL Configuration on AR Series Routers

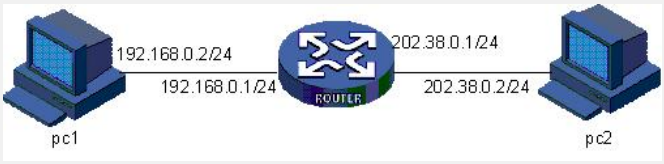
姚忆斌 2007-09-13 发表

Typical Reflexive ACL Configuration on AR Series Routers

[Requirements]

Pc1 accesses the external network through the router. After reflexive ACL is enabled, pc1 initiates a request, and the reply packet of the external network can go into the intranet, but the request initiated by the external network cannot go into the intranet, which is effectively protected against attacks.

[Networking diagram]



[Configuration script]

Configuration script (router)
sysname Quidway # **acl number 3001** **nesting 3000 /Configure the nesting group/** **rule 1 deny ip /Deny all packets/** **acl number 3002** **rule 0 permit ip reflect 3000 timeout 300** **/Configure the reflexive group, and the default aging time for a single item is 300s/** # interface Ethernet0/0 ip address 192.168.0.1 255.255.255.0 # interface Serial1/1 clock DTECLK1 link-protocol ppp ip address 202.38.0.1 255.255.255.0 **firewall packet-filter 3001 inbound /Apply acl3001 in the inbound direction of the interface/** **firewall packet-filter 3002 outbound /Apply acl3002 in the outbound direction of the interface/** # user-interface con 0 user-interface aux 0 user-interface vty 0 4 authentication-mode scheme # return

Set the IP address of pc1 to 192.168.0.2 and that of the gateway to 192.168.0.1.

Set the IP address of pc2 to 202.38.0.2 and that of the gateway to 202.38.0.1.

[Verification]

Execute the **ping 202.38.0.2** command in the dos view on pc1:

Reply from 202.38.0.2: bytes=56 Sequence=1 ttl=127 time=28 ms

Reply from 202.38.0.2: bytes=56 Sequence=2 ttl=127 time=28 ms

Reply from 202.38.0.2: bytes=56 Sequence=3 ttl=127 time=28 ms

Reply from 202.38.0.2: bytes=56 Sequence=4 ttl=127 time=28 ms

Reply from 202.38.0.2: bytes=56 Sequence=5 ttl=127 time=28 ms

Execute the **ping 192.168.0.2** command in the dos view on pc2:

From 202.38.0.1 : Communication Administratively Prohibited

From 202.38.0.1 : Communication Administratively Prohibited

From 202.38.0.1 : Communication Administratively Prohibited

From 202.38.0.1 : Communication Administratively Prohibited

From 202.38.0.1 : Communication Administratively Prohibited

[Tip]

1. Be sure to set the ACL in the inbound direction of the interface denying all access IP packets, which is permitted by default in the system; otherwise, the external networ

k can access the intranet.

2. This function is available on the VRP3.4-E0201 and later versions.