H3C S9500交换机自反ACL配置

刘志伟 2006-12-03 发表

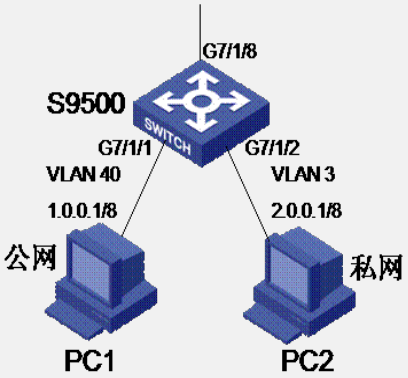
H3C S9500交换机自反ACL配置

一、组网需求:

通过配置自反ACL，达到只有私网访问了公网后才允许公网访问私网，以防止受到外部网络的攻击，保护私网内部的安全。

本实例通过配置合适的ACL及其子规则，完成自反ACL的配置。

二、组网图:



三、配置步骤:

软件版本：S9500交换机E1326软件版本以上

硬件版本：S9500交换机NetStream业务处理板（即LSB1NAMB1）

定义带reflective参数的高级访问控制列表子规则。

<H3C> system-view

[H3C] acl number 3001

[H3C-acl-adv-3001] rule 0 permit udp reflective

[H3C-acl-adv-3001] rule 1 permit tcp reflective

[H3C-acl-adv-3001] rule 2 permit icmp reflective

[H3C-acl-adv-3001] quit

在VLAN 40下配置自反ACL。

[H3C] vlan 40

[H3C-vlan40] packet-filter outbound ip-group 3001 slot 5

[H3C-vlan40] quit

定义用于端口重定向的控制列表子规则。

[H3C] acl number 3002

[H3C-acl-adv-3002] rule 0 permit udp

[H3C-acl-adv-3002] rule 1 permit tcp

[H3C-acl-adv-3002] rule 2 permit icmp

[H3C-acl-adv-3002] quit

在VLAN 40所属端口下配置重定向命令。

[H3C] interface GigabitEthernet 7/1/1

[H3C-GigabitEthernet7/1/1] traffic-redirect inbound ip-group 3002 slot 5 designated-vlan 40

四、配置关键点:

1.自反ACL在NAM和NAT上实现的方式有所区别，本配置在NAM业务板上实现。