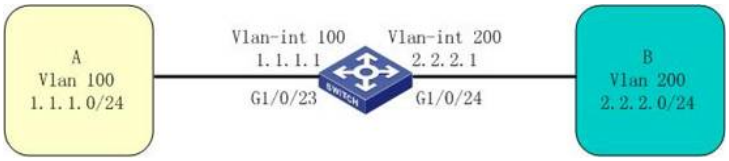
S5500-EI交换机利用ACL实现TCP单向访问的配置

郁啸天【技术大咖】 2009-11-30 发表

S5500-EI交换机利用ACL实现TCP单向访问的配置

一、 组网需求：
2个网段通过一台S5500-EI互联，要求网段A可以访问网段B，网段B不能访问网段A。
二、 组网图：



S5500-EI交换机G1/0/23端口连接Vlan 100，G1/0/24端口连接Vlan 200。
S5500-EI交换机版本必须为R2202P05以上。
三、 配置步骤：
#配置端口、虚接口
[H3C]vlan 100
[H3C-vlan100]port GigabitEthernet 1/0/23
[H3C-vlan100]quit
[H3C]interface Vlan-interface 100
[H3C-Vlan-interface100]ip address 1.1.1.1 24
[H3C-Vlan-interface100]quit
[H3C]vlan 200
[H3C-vlan200]port GigabitEthernet 1/0/24
[H3C-vlan200]quit
[H3C]interface Vlan-interface 200
[H3C-Vlan-interface200]ip address 2.2.2.1 24
#创建ACL，其中第1条匹配TCP连接请求报文，第2条匹配TCP连接建立报文
[H3C]acl number 3001
[H3C-acl-adv-3001]rule 0 permit tcp established source 2.2.2.0 0.0.0.255 destination 1.1.1.0 0.0.0.25
5
[H3C-acl-adv-3001]quit
[H3C]acl number 3002
[H3C-acl-adv-3002]rule 0 permit tcp source 2.2.2.0 0.0.0.255 destination 1.1.1.0 0.0.0.255
#创建流分类，匹配相应的ACL
[H3C]traffic classifier 3001
[H3C-classifier-3001]if-match acl 3001
[H3C-classifier-3001]quit
[H3C]traffic classifier 3002
[H3C-classifier-3002]if-match acl 3002
#创建流行为，permit TCP连接建立报文，deny从 Vlan 200发送的TCP连接建立请求报文
[H3C]traffic behavior 3001
[H3C-behavior-3001]filter permit
[H3C-behavior-3001]quit
[H3C]traffic behavior 3002
[H3C-behavior-3002]filter deny
#创建Qos策略，关联流分类和流行为
[H3C]qos policy 3000
[H3C-qospolicy-3000]classifier 3001 behavior 3001
[H3C-qospolicy-3000]classifier 3002 behavior 3002
#在Vlan 200端口入方向下发Qos策略
[H3C]interface GigabitEthernet 1/0/24
[H3C-GigabitEthernet1/0/24]qos apply policy 3000 inbound

四、 配置关键点：
1. 在配置ACL和Qos策略前必须全网路由可达。如果S5500-EI两端连接的是交换机，则需要配置路由协议或在两端交换机上配置到对方网段的静态路由。
2. 在S5500-EI上配置ACL rule时，tcp established匹配的是带有ack标志位的tcp连接报文，而tcp匹配的是所有tcp连接报文。在配置Qos策略时，匹配流分类和流行为要注意顺序，先匹配permit的，再匹配deny的。这样的结果是在入方向deny了不带有ack标志位的tcp连接报文，其它tcp连接报文均能正常

通过。因此Vlan 200所在网段发起tcp连接时第一个请求报文被deny而无法建立连接，Vlan 100所在网段发起tcp连接时，Vlan 200所在网段发送的都是带有ack标志位的tcp连接报文，连接可以顺利建立。
3. S5500-EI从R2202P05版本开始，在ACL中添加了Established字段，之前的版本无法实现TCP单向访问功能。