V5交换机单向访问配置方法

目录

1 配置需求或说明

1.1适用产品系列

本案例适用于如S3100V2-16TP-EI、S5008PV2-EI、S5120-28P-SI、MS4120-26TP等的V5交换机，V5、V7交换机具体分类及型号可以参考“1.1 Comvare V5、V7平台交换机分类说明”。

1.2配置需求及实现的效果

内网两个网段通过一台交换机互联，出于公司信息安全要求，需要实现主机A可以访问主机B，主机B不能访问主机A。本案例以实现单向访问远程桌面为例。

1.3配置关键点

在交换机上配置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。因此主机B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，主机A所在网

段发起tcp连接时，主机B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。

2 组网图

3 配置步骤

3.1配置步骤

#配置接口地址（此处省略）

#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 3000
[H3C-acl-adv-3000]rule 0 permit tcp established
source 192.168.20.0 0.0.0.255 destination
192.168.10.0 0.0.0.255
[H3C-acl-adv-3000]quit
[H3C]acl number 3200
[H3C-acl-adv-3200]rule 0 permit tcp source
192.168.20.0 0.0.0.255 destination 192.168.10.0
0.0.0.255
```

#创建流分类，匹配相应的ACL

```
[H3C]traffic classifier 1
```

```
[H3C-classifier-1]if-match acl 3100
[H3C-classifier-1]quit
[H3C]traffic classifier 2
[H3C-classifier-2]if-match acl 3200
```

#创建流行为，permit TCP连接建立报文，deny从 Vlan 20发送到vlan10的TCP连接建立请求报文

```
[H3C]traffic behavior 11
[H3C-behavior-11]filter permit
[H3C-behavior-3]quit
[H3C]traffic behavior 22
[H3C-behavior-22]filter deny
```

#创建Qos策略，关联流分类和流行为

```
[H3C]qos policy 3
[H3C-qospolicy-3]classifier 1 behavior 11
[H3C-qospolicy-3]classifier 2 behavior 22
```

#在Vlan 20端口入方向下发Qos策略

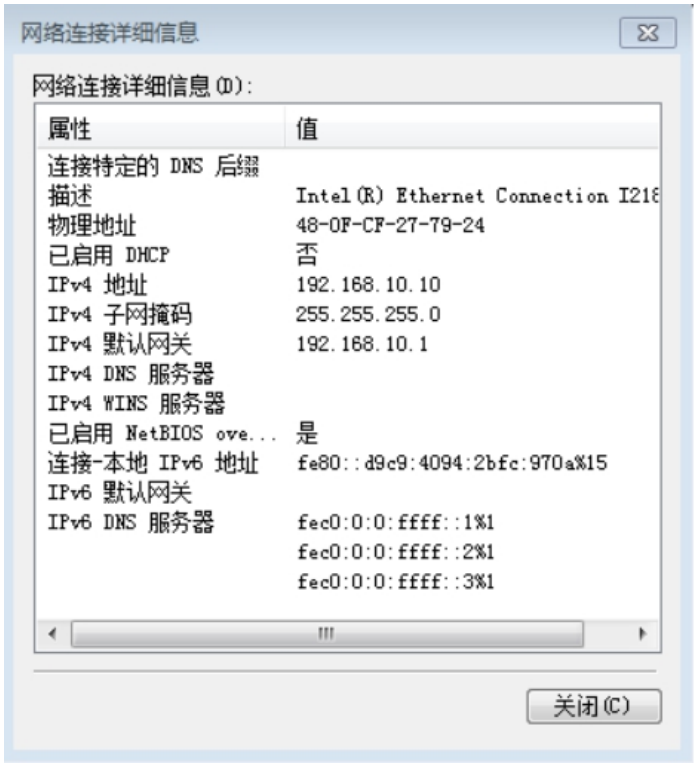
```
[H3C]interface GigabitEthernet 1/0/20
[H3C-GigabitEthernet1/0/20]qos apply policy 3 inbound
```

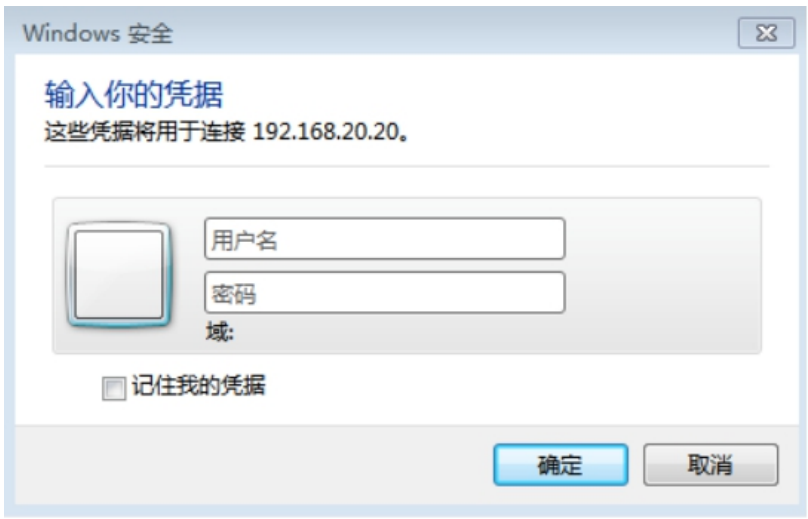
#保存配置

```
[H3C]save force
```

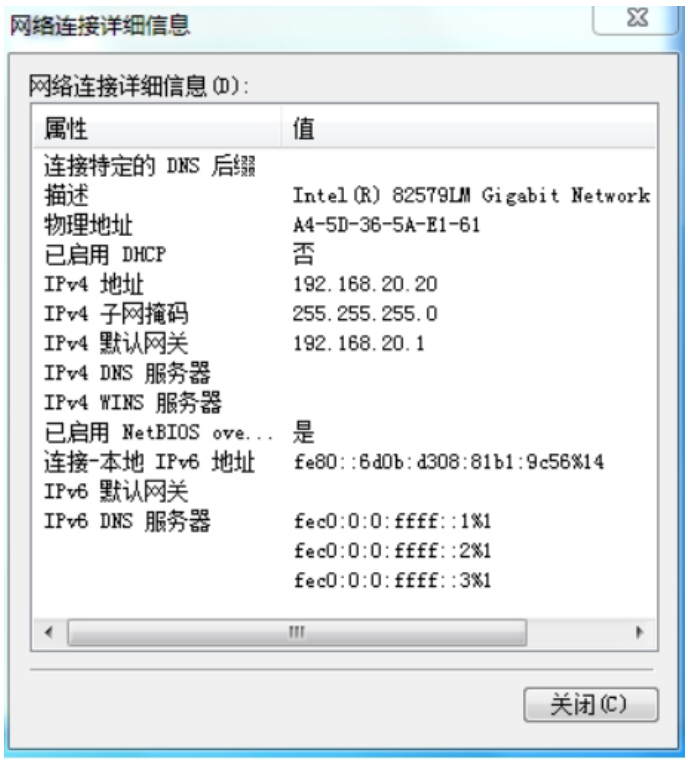
3.2 配置验证

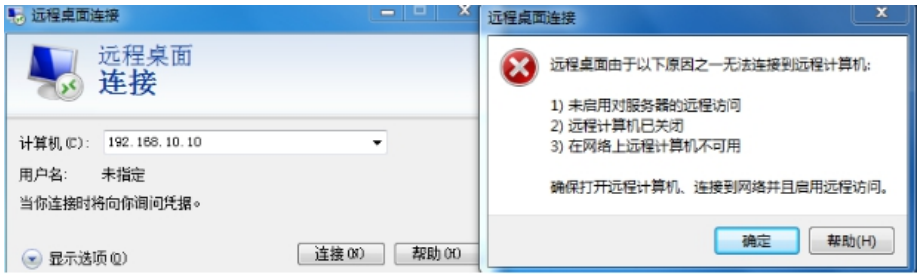
PC1可以远程桌面PC2：





PC2无法远程桌面PC1


网络连接详细信息
网络连接详细信息(D):
属性
值
连接特定的 DNS 后缀
描述
Intel(R) 82579LM Gigabit Network
物理地址
A4-5D-36-5A-E1-61
已启用 DHCP
否
IPv4 地址
192.168.20.20
IPv4 子网掩码
255.255.255.0
IPv4 默认网关
192.168.20.1
IPv4 DNS 服务器
IPv4 WINS 服务器
已启用 NetBIOS ove...
是
连接-本地 IPv6 地址
fe80::6d0b:d308:81b1:9c56%14
IPv6 默认网关
IPv6 DNS 服务器
fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
关闭(C)


远程桌面连接
远程桌面
连接
计算机(C): 192.168.10.10
用户名: 未指定
当你连接时将向你询问凭据。
显示选项(O)
连接(N)
帮助(H)
远程桌面连接
远程桌面由于以下原因之一无法连接到远程计算机:
1) 未启用对服务器的远程访问
2) 远程计算机已关闭
3) 在网络上远程计算机不可用
确保打开远程计算机、连接到网络并且启用远程访问。
确定
帮助(H)