

知 S6X00系列交换机单向访问配置方法

ACL QoS Godiva612 2018-11-28 发表

组网及说明

1.1适用产品系列

本案例适用于如S6300-52QF、S6520X-30QC-HI、S6800-54QT、S6820-4C S6900-2F等S6X00系列的交换机。

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



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 advanced 3100
```

```
[H3C-acl-ipv4-adv-3100]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-ipv4-adv-3100]quit
```

```
[H3C]acl advanced 3200
```

```
[H3C-acl-ipv4-adv-3200]rule 0 permit tcp source 192.168.20.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
```

```
[H3C-acl-ipv4-adv-3200]quit
```

#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-3000]classifier 2 behavior 22
```

#在Vlan 20端口入方向下发Qos策略

```
[H3C]interface GigabitEthernet 1/0/20
```

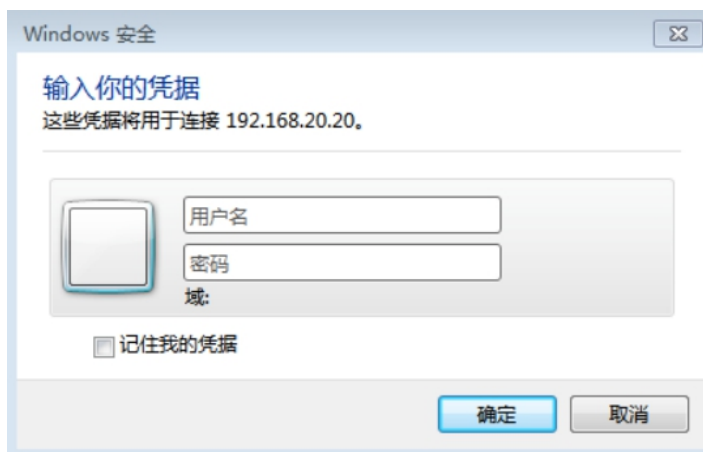
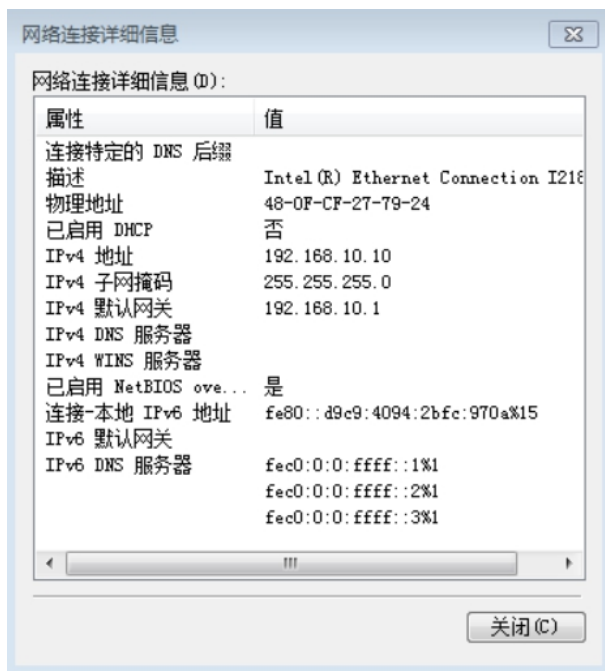
```
[H3C-GigabitEthernet1/0/20]qos apply policy 3 inbound
```

#保存配置

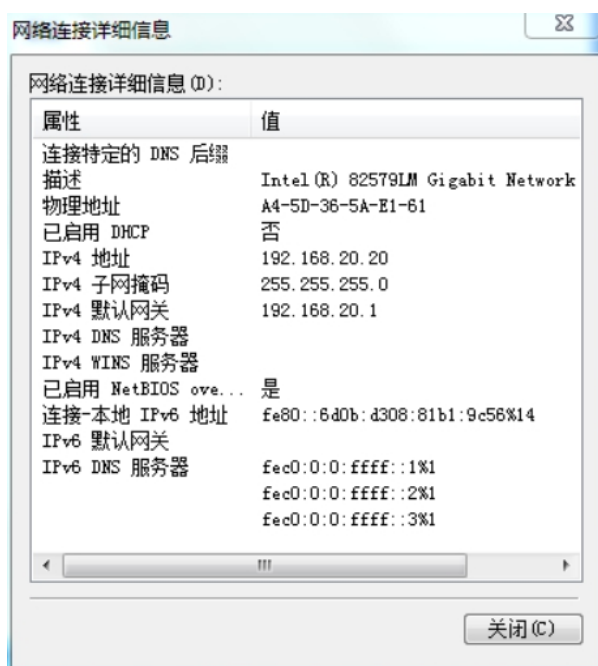
```
[H3C]save force
```

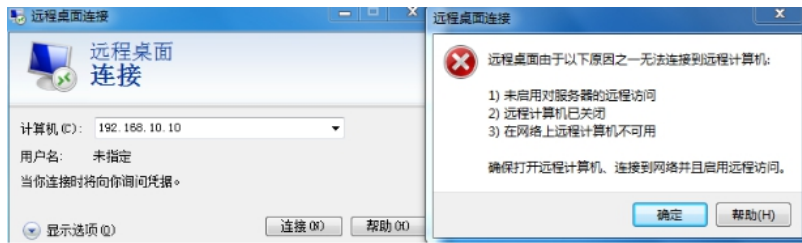
3.2 配置验证

PC1可以远程桌面PC2:



PC2无法远程桌面PC1





配置关键点