

知 S5500/S5800/S5830系列交换机拒绝指定的主机访问网络配置方法（命令行版）

packet-filter 夏威 2018-11-24 发表

组网及说明

1 配置需求或说明

1.1 适用产品系列

本案例适用于如S5500-20TP-SI、S5500-52C-EI、S5500-52C-PWR-EI、S5500-34C-HI、S5800-32C-EI、S5800-32F、S5800-60C-PWR、S5830-106S等S5500、S5800、S5830系列的交换机。

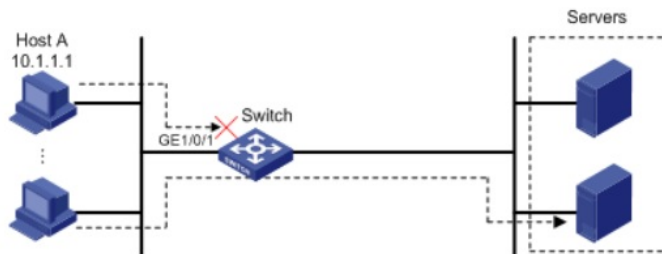
1.2 配置注意事项

对于未匹配ACL规则的报文，包过滤功能采取允许通过的动作。

1.3 配置需求及实现的效果

Host A和其它主机通过端口GigabitEthernet 1/0/1接入交换机，Host A的IP地址为10.1.1.1。要求通过配置ACL，实现在GigabitEthernet1/0/1端口上拒绝Host A发送的报文通过，允许来自其它主机的报文通过。

2 组网图



配置步骤

3 配置步骤

3.1 配置步骤

创建IPv4基本ACL 2000，配置拒绝源IP地址为10.1.1.1的报文通过的规则。

```
[H3C] acl number 2000
```

```
[H3C-acl-basic-2000] rule deny source 10.1.1.1 0
```

```
[H3C-acl-basic-2000] quit
```

配置包过滤功能，应用IPv4基本ACL 2000对端口GigabitEthernet1/0/1收到的IPv4报文进行过滤。

```
[H3C] interface gigabitethernet 1/0/1
```

```
[H3C-GigabitEthernet1/0/1] packet-filter 2000 inbound
```

3.2 验证配置

执行display packet-filter命令查看包过滤功能的应用状态。

```
[H3C] display packet-filter interface GigabitEthernet 1/0/1
```

```
Interface: GigabitEthernet1/0/1
```

```
In-bound Policy:
```

```
acl 2000, Successful
```

上述信息显示GigabitEthernet1/0/1端口上已经正确应用了包过滤功能。

在除HostA的其它主机上以图中右侧任意一台服务器为目的进行ping操作，返回正常应答信息；在Host A上执行此操作返回请求超时信息，在所有主机上执行此操作均能返回正常应答信息。

4 保存设备配置

```
[H3C] save force
```

配置关键点