# S3600高危端口封堵配置案例

ACL 韦家宁 2020-09-18 发表

## 组网及说明

为了进一步保证设备安全，需配置ACL对高危端口进行拦截。

S3600的版本信息如下：

```
H3C Comware Platform Software
Comware Software, Version 5.20, Release 2112
Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.
H3C S3600V2-28TP-EI uptime is 2 weeks, 1 day, 20 hours, 48 minutes

H3C S3600V2-28TP-EI with 1 Processor
256M    bytes SDRAM
2M      bytes Nor Flash Memory
128M    bytes Nand Flash Memory
Config Register points to Nand Flash

Hardware Version is Ver.A
CPLD Version is 001
BootRom Version is 133
[SubSlot 0] 24FE+4SFP+2Combo GE Hardware Version is Ver.A
```

## 配置步骤

1、创建ACL，对高危端口进行拦截：

```
acl number 3210
 rule 0 deny tcp destination-port eq 135
 rule 1 deny udp destination-port eq 135
 rule 2 deny tcp destination-port eq 137
 rule 3 deny udp destination-port eq netbios-ns
 rule 4 deny tcp destination-port eq 138
 rule 5 deny udp destination-port eq netbios-dgm
 rule 6 deny udp destination-port eq netbios-ssn
 rule 7 deny tcp destination-port eq 139
 rule 8 deny tcp destination-port eq 445
 rule 9 deny udp destination-port eq 445
 rule 10 deny tcp destination-port eq 3389
 rule 11 deny udp destination-port eq 3389
 rule 20 deny tcp source-port eq 135
 rule 21 deny udp source-port eq 135
 rule 22 deny tcp source-port eq 137
 rule 23 deny udp source-port eq netbios-ns
 rule 24 deny tcp source-port eq 138
 rule 25 deny udp source-port eq netbios-dgm
 rule 26 deny udp source-port eq netbios-ssn
 rule 27 deny tcp source-port eq 139
 rule 28 deny tcp source-port eq 445
 rule 29 deny udp source-port eq 445
 rule 30 deny tcp source-port eq 3389
 rule 31 deny udp source-port eq 3389
 rule 1500 permit ip
```

2、将ACL下发到端口：

```
int  Ethernet 1/0/1
packet-filter 3210 inbound
packet-filter 3210 outbound
quit
```

## 配置关键点