S5560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

本案例为S5560部署ACL来对高危端口进行封堵。

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 range gi 1/0/1 gi 1/0/24
packet-filter 3210 inbound
packet-filter 3210 outbound
quit
```

配置关键点