F1060防火墙使用ACL拦截高危端口案例

ACL 韦家宁 2020-09-20 发表

组网及说明

本案例使用F1060防火墙的ACL对高危端口进行拦截。

F1060版本信息如下：

<H3C>dis version

H3C Comware Software, Version 7.1.064, Alpha 7164

H3C SecPath F1060 uptime is 0 weeks, 0 days, 0 hours, 16 minutes

Last reboot reason: User reboot

Boot image: flash:/sim_f1000_fw-cmw710-boot-a6401.bin

Boot image version: 7.1.064, Alpha 7164

Compiled Sep 18 2017 16:00:00

Boot image: flash:/sim_f1000_fw-cmw710-system-a6401.bin

Boot image version: 7.1.064, Alpha 7164

Compiled Sep 18 2017 16:00:00

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 gi 1/0/1

packet-filter 3210 inbound

packet-filter 3210 outbound

quit

配置关键点