用户登录权限配置方法

其他 WEB管理 张新姿 2020-09-28 发表

组网及说明

1 配置需求或说明

1.1 适用的产品系列

本案例适用于软件平台为Comware V7系列防火墙：如M9006、M9010、M9014等M9K系列的防火墙。

注：本案例是在F1000-C-G2的Version 7.1.064, Release 9323P1801版本上进行配置和验证的。

1.2 配置需求及实现的效果

根据网络安全规定用户通过SSH、Telnet、Console口登录设备后操作权限有如下限制：

1. 不允许用户登录后对admin账号进行修改操作；
2. 不允许用户登录后在全局或者接口执行undo、reset、shutdown、save等高危命令；

3、不允许用户执行所有三层协议相关功能的命令；

除了上述三点限制外用户可以对执行其他命令；

配置步骤

1 配置步骤

1.1 配置角色策略

#新建角色名称为“test”

system-view

[H3C]role name test

#最后一条所有命令均允许；

[H3C-role-test] rule 10 permit command *

#拒绝用户在接口下执行shutdown命令；

[H3C-role-test] rule 20 deny command system-view ; interface * ; shutdown

#拒绝用户执行执行reset命令；

[H3C-role-test] rule 30 deny command reset *

#拒绝用户在全局下执行undo命令；

[H3C-role-test] rule 40 deny command system-view ; undo *

#拒绝用户在接口下执行undo命令；

[H3C-role-test] rule 50 deny command system-view ; interface * ; undo *

#拒绝用户执行save命令；

[H3C-role-test] rule 60 deny command save *

#拒绝用户执行关于设备三层协议的所有命令；

[H3C-role-test] rule 70 deny write feature-group L3

1.2 在用户下调用角色test策略

#使用超级管理员账号创建用户名为aaa的账号

system-view

[H3C]local-user aaa

[H3C-luser-manage-aaa]password simple XXXXXXX

[H3C-luser-manage-aaa] service-type telnet

[H3C-luser-manage-aaa] authorization-attribute user-role test

[H3C-luser-manage-aaa] undo authorization-attribute user-role network-operator

[H3C-luser-manage-aaa] quit

2 功能测试

1. 不允许用户登录后对admin账号进行修改操作；

Login: aaa

Password:

system-view

[H3C]local-user 123

Insufficient right to perform the operation. \\无法进入其他用户视图

[H3C]local-user admin

Insufficient right to perform the operation. \\无法进入admin用户视图

[H3C]local-user aaa

[H3C-luser-manage-aaa] password simple 123456 \\可以进入本用户视图

2. 不允许用户登录后在全局或者接口执行undo、reset、shutdown、save等高危命令；

saved-configuration \\重置配置被拒绝

Permission denied.

reset counters interface \\清空接口统计被拒绝

Permission denied.

[H3C]undo ssh server enable　　\\删除SSH服务被拒绝
Permission denied.
save　　\\保存配置和强制保存均被拒绝
Permission denied.
save f
Permission denied.

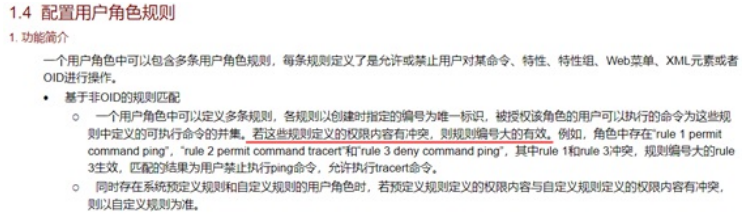
3. 不允许用户执行所有三层协议相关功能的命令；

system-view　　\\创建OSPF进程被拒绝
[H3C]ospf 1
Permission denied.

配置关键点

注意事项

1. 不允许用户登录后对admin账号进行修改操作；
   缺省情况下仅network-admin或者level-15角色的用户具有执行创建/修改/删除所有本地用户和本地用户组的权限，使用其他角色用户只能对本用户内容进行编辑无法编辑其他用户配置，因此第一个需求只需要新建账号不具有network-admin或者level-15角色即可。
1. 不允许用户登录后在全局或者接口执行undo、reset、shutdown、save等高危命令；
   1）角色规则中是按照角色编号越大越优先执行的逻辑，因此配置只有某些命令不执行而其他命令均可以执行需求时，要求全放通策略规则编号比其他规则编号小；


1.4 配置用户角色规则

1. 功能简介

一个用户角色中可以包含多条用户角色规则，每条规则定义了是允许或禁止用户对某命令、特性、特性组、Web菜单、XML元素或者OID进行操作。

- 基于非OID的规则匹配
  - 一个用户角色中可以定义多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则中定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，角色中存在"rule 1 permit command ping"，"rule 2 permit command tracert"和"rule 3 deny command ping"，其中rule 1和rule 3冲突，规则编号大的rule 3生效，匹配的结果为用户禁止执行ping命令，允许执行tracert命令。
  - 同时存在系统预定义规则和自定义规则的用户角色时，若预定义规则定义的权限内容与自定义规则定义的权限内容有冲突，则以自定义规则为准。

2. 2）对于“shutdown”、“undo”等命令需要注意命令所在的视图执行，举例“shutdown”一般在接口视图下执行，因此规则配置为system-view ; interface * ; shutdown，其中“;”表示视图。
   3、不允许用户执行所有三层协议相关功能的命令；
   缺省情况下，特性组存在两个系统预定义特性组，名称为L2和L3，且不能被修改和删除。其中L3特性组中包含了所有与路由等三层协议相关的命令；

```
[HZB7-R1-F1060-IRF]display role feature-group
Feature group: L2
Feature: igmp-snooping    (IGMP-Snooping related commands)
Feature: mld-snooping     (MLD-Snooping related commands)
Feature: lacp             (LACP related commands)
Feature: stp              (STP related commands)
Feature: lldp             (LLDP related commands)
Feature: dldp             (DLDP related commands)
Feature: smart-link       (Smart-link related commands)
Feature: monitor-link     (Monitor-link related commands)
Feature: loopbk-detect    (Loopback-detection related commands)
Feature: vlan             (Virtual LAN related commands)
Feature: evb              (EVB related commands)
Feature: ofp              (OFP related commands)

Feature group: L3
Feature: route            (Route management related commands)
Feature: usr              (Unicast static route related commands)
Feature: ospf             (Open Shortest Path First protocol related commands)
Feature: rip              (Routing Information Protocol related commands)
Feature: isis             (ISIS protocol related commands)
Feature: bgp              (Border Gateway Protocol related commands)
Feature: l3vpn            (Layer 3 Virtual Private Network related commands)
Feature: route-policy     (Routing Policy related commands)
Feature: multicast        (Multicast related commands)
Feature: pim              (Protocol Independent Multicast related commands)
Feature: igmp             (Internet Group Management Protocol related commands)
Feature: mld              (Multicast Listener Discovery related commands)
```

4、创建本地用户时默认会生成“authorization-attribute user-role network-operator”命令，需要将其删除后再添加需要的角色策略；