某局点F1020防火墙增加VPN配置后无法登陆经典案例

WEB管理 其他 李波 2021-01-29 发表

组网及说明

不涉及

问题描述

某局点做完VPN相关配置之后，使用SSH，WEB，console登陆F1020防火墙时均提示登录失败

过程分析

1、由于无法登录设备收集信息，建议先跳过配置或者console密码登录，重启设备（在确认不影响业务的情况下）进入boot菜单

```
==========================<EXTENDED-BOOTWARE MENU>==========================
|<1> Boot System |
|<2> Enter Serial SubMenu |
|<3> Enter Ethernet SubMenu |
|<4> File Control |
|<5> Restore to Factory Default Configuration |
|<6> Skip Current System Configuration |
|<7> BootWare Operation Menu |
|<8> Skip Authentication for Console Login |
|<9> Storage Device Operation |
 |<0> Reboot |
==============================================================================
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+C: Display Copyright
Ctrl+F: Format File System
Enter your choice(0-9): 8
Clear Image Password Success!
```

按“6”跳过配置登录设备，按“8”跳过console密码登录设备

2、登录后将之前配置信息导出

发现客户新增了vpn的domain

```
# domain vpn authorization-attribute idle-cut 15 10240
 authorization-attribute ip-pool radius
 authentication ppp radius-scheme vpn
 authorization ppp radius-scheme vpn
 accounting ppp radius-scheme vpn
 authentication default radius-scheme vpn
 accounting default radius-scheme vpn
#
```

并且将vpn设置为默认domain

```
 domain default enable vpn
```

这种情况下，登录设备时进行认证的域就变成了vpn域，如果没有指定相关service-type的认证方式，那么认证方式缺省就是local，也就是登录只需要在本地进行认证即可

但是现场又使用了以下命令

```
 authentication default radius-scheme vpn
 accounting default radius-scheme vpn
```

这两条命令将所有service-type的认证方式设置为radius-scheme

也就是需要进行AAA认证，认证成功才能登录，而radius服务器上并没有相关的设置，所以登录也就失败了

解决方法

1、将缺省域改为system域，vpn的账户在登录是增加后缀名@vpn

2、将vpn域的缺省认证方式改为local，或者将vpn域关于login的认证方式改为local，登录设备在本地进行认证