

知 SecPath F1000-AI-15(V7) 通过带内地址登录web失败

WEB管理 贾珊珊 2023-08-29 发表

组网及说明

不涉及

问题描述

现场通过带内管理地址登录防火墙web显示登录失败，通过带外管理口使用相同的账号密码可以登录上去

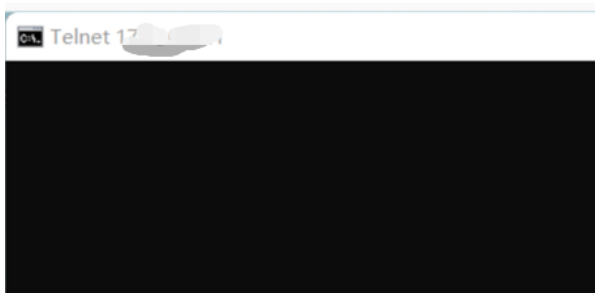


过程分析

检查现场的配置，接口下开启的http登录，安全策略也放通了，telnet+443端口也可以上去

```
port link-mode route
#
interface GigabitEthernet1/0/8
port link-mode route
ip address 192.168.1.3
manage http inbound
manage https inbound
manage https outbound
manage netconf-http inbound
manage netconf-https inbound
manage netconf-ssh inbound
manage ssh inbound
#
```

```
destination-zone Local
rule 25 name 内网主机
action pass
source-zone Trust
source-zone Local
destination-zone Local
destination-zone Trust
rule 26 name 主机上网-同步授权
```



在防火墙上开启debugging local-server all存在如下报错：

```
*Jul 16 03:17:18:857 2023 FW LOCALSER/7/EVENT: Received authentication request message.
```

```
*Jul 16 03:17:18:858 2023 FW LOCALSER/7/EVENT: Authentication failed, unexpected user service type 1024 (expected = 2208).
```

从debug信息可以看出是用户服务不匹配导致的登录不上，检查现场的用户配置如下：

```
#
local-user XXXX class manage
password hash YYYYYY
service-type ssh terminal https
authorization-attribute user-role level-15
authorization-attribute user-role network-operator
#
```

解决方法

从报错截图可以看到，登录界面也是https，看着没有问题，但经确认，通过带内管理访问时，现场用的是http，由于页面输入密码需要加密，因此 http打开会重定向到https，认证通过后会变回http。最后在用户下的service-type增加http后问题解决

