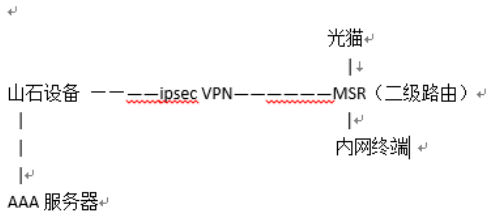
MSR SSH结合HWTACACS 认证成功，但是命令行输入没有权限

Tacacs　徐宁　2020-07-06 发表

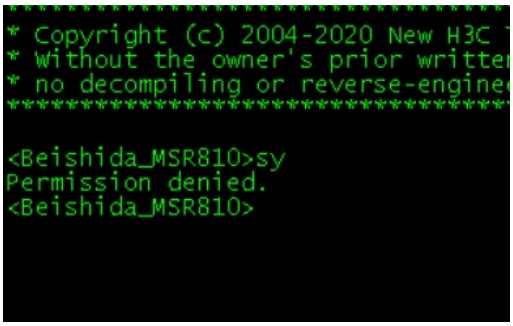
组网及说明

MSR侧内网终端通过ipsec隧道访问AAA服务器，从而实现认证，组网如下：



问题描述

目前配置完成后，客户在MSR侧内网可以访问到服务器，认证也是通过的，但是认证成功后登录设备，命令行输入提示没有权限



过程分析

开始设备配置如下：

```
# line vty 0 4
 authentication-mode scheme
 user-role network-admin
 protocol inbound ssh
 idle-timeout 30 0
 command authorization
 command accounting
#
 line vty 5 15
 authentication-mode scheme
 user-role network-admin
 protocol inbound ssh
 command authorization
 command accounting
# hwtacacs scheme acs
 primary authentication 192.168.X.X
 primary authorization 192.168.X.X
 primary accounting 192.168.X.X
 key authentication cipher
 key accounting cipher
 user-name-format without-domain
# domain acs authentication
login hwtacacs-scheme acs local authorization
login hwtacacs-scheme acs local accounting
login hwtacacs-scheme acs local
#
```

发现在用户线下配置了command authorization，开启命令行授权功能后，使用该用户线登录的用户只能执行服务器授权的命令，服务器没有授权的命令不能执行。所以需要在domin下配置authorization command hwtacacs-scheme

解决方法

在domin下配置authorization command hwtacacs-scheme后问题解决