

SecPath1800F对console口登陆用户做RADIUS认证功能的配置

一、组网需求:

Secpath1800F在console口上使用RADIUS认证以保证链接的安全性

二、组网图:



三、配置步骤:

适用版本：所有Secpath1800F VRP版本

```
sysname Secpath1800F
#
firewall packet-filter default permit interzone local trust direction inbound
firewall packet-filter default permit interzone local trust direction outbound
firewall packet-filter default permit interzone local untrust direction inbound
firewall packet-filter default permit interzone local untrust direction outbound
firewall packet-filter default permit interzone local dmz direction inbound
firewall packet-filter default permit interzone local dmz direction outbound
firewall packet-filter default permit interzone trust untrust direction inbound
firewall packet-filter default permit interzone trust untrust direction outbound
firewall packet-filter default permit interzone trust dmz direction inbound
firewall packet-filter default permit interzone trust dmz direction outbound
firewall packet-filter default permit interzone dmz untrust direction inbound
firewall packet-filter default permit interzone dmz untrust direction outbound
#
firewall mode route
#
firewall statistic system enable
#
#
radius-server template shiva // 配置服务器模板
radius-server shared-key pass // 配置服务器验证密码
radius-server authentication 1.1.1.3 1812 // 配置服务器的ip地址及端口
#
interface Aux0
  async mode flow
  link-protocol ppp
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet1/0/0
#
interface Ethernet1/0/1
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
```

```

#
interface Ethernet1/0/4
#
interface Ethernet1/0/5
#
interface Ethernet1/0/6
#
interface Ethernet1/0/7
ip address 1.1.1.1 255.255.255.0
#
interface NULL0
#
firewall zone local
set priority 100
#
firewall zone trust
set priority 85
add interface Ethernet1/0/7
#
firewall zone untrust
set priority 5
#
firewall zone dmz
set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local dmz
#
firewall interzone trust untrust
#
firewall interzone trust dmz
#
firewall interzone dmz untrust
#
aaa
authentication-scheme default
authentication-scheme radius // 配置用来验证的 scheme
authentication-mode radius // 配置scheme相应的验证模式
#
authorization-scheme default
#
accounting-scheme default
#
domain default
domain huawei // 配置huawei域验证的scheme 及认证服务器
authentication-scheme radius
radius-server shiva
#
#
user-interface con 0 // 指定console的验证方式为 aaa
authentication-mode aaa
user-interface aux 0
user-interface vty 0 4
authentication-mode none
user privilege level 3
#
return

```

四、配置关键点:

验证时输入用户名指明是huawei域, 格式如 [test@huawei](#)

当与CAMS做交互认证时，如果需要对用户授权，则在CAMS选择权限级别时不能大于

3，否则会导致权限不能正常下发。