

思科认证:CCIE安全认证学习笔记 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/142/2021\\_2022\\_\\_E6\\_80\\_9D\\_E7\\_A7\\_91\\_E8\\_AE\\_A4\\_E8\\_c101\\_142389.htm](https://www.100test.com/kao_ti2020/142/2021_2022__E6_80_9D_E7_A7_91_E8_AE_A4_E8_c101_142389.htm) # aaa new-model 打开aaa服务

# aaa authentication login 4sec tacacs local 告诉路由器先用tacacs 校验用户，如果tacacs服务器报告出错（比如tacacs服务器没有打开）就用路由器本地用户校验登录。如果tacacs服务器拒绝用户登录，则不会用路由器本地用户校验登录。

# aaa authorization exec default tacacs local 该命令告诉路由器使用tacacs服务器检验用户权限，如果tacacs服务器报错则用路由器本地设置检验用户权限。 # aaa authorization commands 4

4sec tacacs 该命令在此处无效，因为没有让vty 0 4用list 4sec来校验权限。如果此处把命令改为：aaa authorization commands 4

default group tacacs 则路由器会用tacacs服务器来校验每一个

权限高于4的命令。如果把命令改为：aaa authorization commands 4 default group tacacs local虽然路由器还是会用tacacs

服务器来校验每一个权限高于4的命令，但是一旦tacacs出错，我们还是可以通过路由器的本地用户及权限来登录并修正

错误。如果把命令改为：aaa authorization commands 4 default group tacacs local none则用户在tacacs服务器停止工作和没有本地用户名一样可以登录路由器。

# username fumtek privilege 7 password 0 password 该命令设置用户fumtek的密码 # username admin privilege 15 password 0 passpass 该命令设置管理员的密码

# tacacs-server host 10.10.10.10 指定tacacs服务器的地址

# tacacs-server key key4sec 指定NAS和tacacs服务器之间密码交换是的密钥。 line vty 0 4 login authentication 4sec exec-timeout 0

```
0 RouterA crypto isakmp policy 100 crypto isakmp key seckey
address 216.12.12.2 !! crypto ipsec transform-set 4sec esp-des
esp-sha-hmac ! crypto map 4sec 100 ipsec-isakmp set peer
216.12.12.2 set transform-set 4sec set pfs group1 match address 100 !
interface Serial0/0 ip address 216.12.12.1 255.255.255.252 crypto
map 4sec ! access-list 100 permit ip 10.10.10.0 0.0.0.255 20.20.20.0
0.0.0.255 !
```

```
-----
RouterB crypto isakmp policy 100 crypto isakmp key seckey address
216.12.12.1 !! crypto ipsec transform-set 4sec esp-des esp-sha-hmac
! crypto map 4sec 100 ipsec-isakmp set peer 216.12.12.1 set
transform-set 4sec set pfs group1 match address 100 ! interface
Serial0/0 ip address 216.12.12.2 255.255.255.252 crypto map 4sec !
access-list 100 permit ip 20.20.20.0 0.0.0.255 10.10.10.0 0.0.0.255 !
```

分析：由于此处没有设置ISAKMP的选项，所以会用默认值。  
ISAKMP的默认值是：加密法则：DES 56bit Hash法则：SHS  
鉴别方法：RSAS Diffe-Hellman组：# 1（768bit）生命期限  
：86400秒 ISAKMP的各种设定值有：加密法则：DES（56bit  
）和3DES（168bit）Hash法则：md5和sha 鉴别方法  
：pre-share, rsa-encr, rsa-sig Diffie-Hellman组：Diffie-Hellman  
group 1(768bit)和Diffie-Hellman group 1(1024bit)生命期限：60  
~ 86400秒 100Test 下载频道开通，各类考试题目直接下载。  
详细请访问 [www.100test.com](http://www.100test.com)