

AR系列路由器使用SSH用户验证方式为RSA登录路由器的典型配置

【需求】

SSH是Secure Shell（安全外壳）的简称，用户通过一个不能保证安全的网络环境远程登录到路由器时，SSH特性可以提供安全保障和强大的认证功能，以保护路由器不受诸如IP地址欺诈、明文密码截取等等的攻击。

使用SSH Client通过RSA方式登录路由器

【配置】

```

配置脚本
#
sysname Quidway
#
radius scheme system
#
domain system
#
rsa peer-public-key huawei          /进入公共密钥视图/
public-key-code begin              /进入公共密钥编辑视图/
308186
028180
9140F8A0 46F74132 E712E3D6 CCFDD706 84ABFD68 CFDD22DC 4A18AD6D 6
BBDB413
58A635F9 85A87BB5 C58EFC3A 7FEC9089 68594BDD 60450712 7AB7D5BB A1
104DBF
D39F17B8 2981EEE8 5D703B2A CE439C93 02C3D8CC C9434209 335430AC D
CC06A0A
C335586C 088D82FE FD07E624 D715BB07 3A46549B 57F649E7 6A276750 741
CF8EB
0201
25
/贴入预先生成的RSA公钥,参考附录来生成该公钥/
public-key-code end                /退出公共密钥编辑视图/
peer-public-key end                /退出公共密钥视图/
#
local-user huawei                   /创建本地帐号=huawei,密码=huawei,类型为ssh,级
别为3/
password simple huawei
service-type ssh
level 3
#
interface Ethernet1/0/0
ip address 192.168.1.1 255.255.255.0
#
interface NULL0
#
ssh user huawei assign rsa-key huawei /为用户指定使用的RSA密钥/
ssh user huawei authentication-type RSA /配置SSH用户验证方式为rsa/
ssh user huawei service-type stelnet /配置SSH用户服务类型为stelnet/
#
user-interface con 0
user-interface vty 0 4
authentication-mode scheme
#
return

```

【验证】

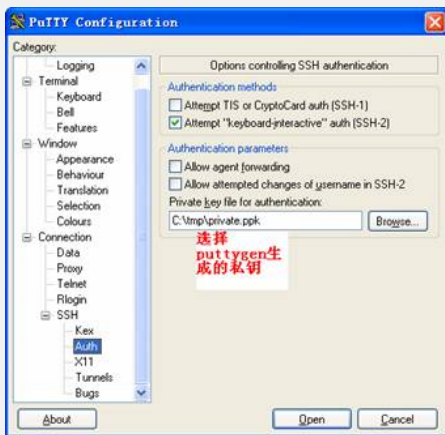
1、生成本地RSA主机密钥对和服务器密钥对

```

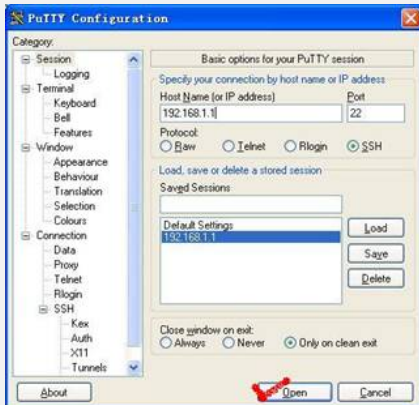
[Quidway]rsa local-key-pair create
The key name will be: Quidway_Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
      It will take a few minutes.
Input the bits in the modulus[default = 512]: /主机密钥的缺省位数为512位/
Generating keys...
.....+++++++
+++++++
.....+++++++
.....+++++++

```

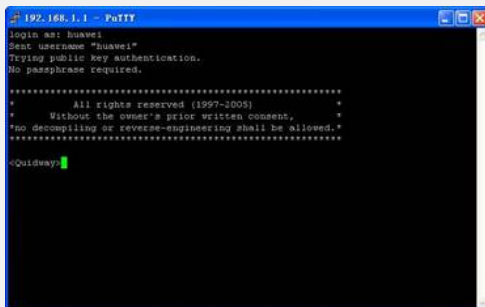
2、使用putty软件，使用通过puttygen生成的私钥进行验证



3、指定地址，建立SSH连接



4、输入账号，不需要输入密码即可登录

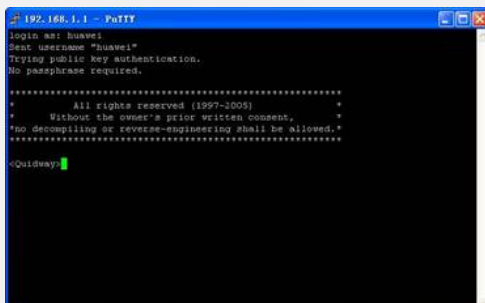


【提示】

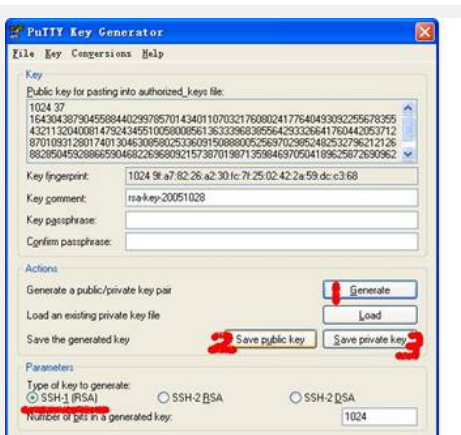
- 1、以上提到的软件在论坛上都可以下载到：
<http://forum.viewthread.php?tid=17170&page=1&extra=#pid99343>

【附录：密钥生成和转换】

- 1、使用puttygen生成公钥和私钥对，并分别保存



- 2、使用SSHkey对生成的公钥进行格式转换



3. 将生成的公钥配置在路由器上