设备管理-SSH登陆设备配置方法

目录

1 配置需求或说明

1.1 适用的产品系列

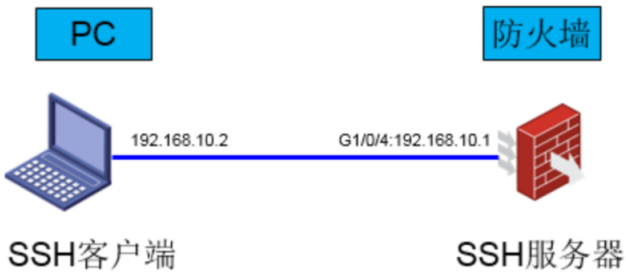
本案例适用于软件平台为Comware V7系列防火墙：F100-X-G2、F1000-X-G2、F100-WiNet、F1000-AK、F10X0等

注：本案例是在F1000-C-G2的Version 7.1.064, Release 9323P1801版本上进行配置和验证的。

1.2 配置需求及实现的效果

用户可以通过电脑上运行的SSH客户端软件（SSH2版本）安全地登录到Device上，并被授予用户角色network-admin进行配置管理；设备采用password认证方式对SSH客户端进行认证，客户端的用户名和密码保存在本地。

2 组网图



3 配置步骤

3.1 配置SSH服务器

```
#进入系统视图
<H3C>system-view
# 生成RSA密钥对，在提示“Y/N”的时候选择“Y”。
[H3C]public-key local create rsa
The local key pair already exists.
Confirm to replace it? [Y/N]:y
The range of public key modulus is (512 ~
2048).
If the key modulus is greater than 512, it
will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys....
Create the key pair successfully.
# 生成DSA密钥对
[H3C]public-key local create dsa
The range of public key modulus is (512 ~
```

```
2048).
If the key modulus is greater than 512, it
will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys.....
Create the key pair successfully.
```

开启SSH服务器功能

```
[H3C]ssh server enable
```

配置接口GigabitEthernet1/0/4的IP地址，客户端将通过该地址连接SSH服务器。

```
[H3C]interface GigabitEthernet1/0/4
[H3C-GigabitEthernet1/0/4]ip address
192.168.10.1 255.255.255.0
[H3C-GigabitEthernet1/0/4]quit
```

设置SSH客户端登录用户线的认证方式为AAA认证。

```
[H3C]line vty 0 63
[H3C-line-vty0-63]authentication-mode scheme
[H3C-line-vty0-63]quit
```

创建设备管理类本地用户为admin，密码为admin；并设置服务类型为SSH，用户角色为network-admin。

```
[H3C]local-user admin
[H3C-luser-manage-admin]service-type ssh
[H3C-luser-manage-admin]authorization-
attribute user-role network-admin
[H3C-luser-manage-admin]password simple
admin
[H3C-luser-manage-admin]quit
```

3.2 防火墙域间策略配置

```
# 把接口GigabitEthernet1/0/1加入trust区域
[H3C]security-zone name Trust
[H3C-security-zone-Trust]import interface
GigabitEthernet1/0/1
[H3C-security-zone-Trust]quit
```

#创建对象策略pass。

```
[H3C]object-policy ip pass
[H3C-object-policy-ip-pass] rule 0 pass
[H3C-object-policy-ip-pass]quit
```

#创建Trust到Local域的域间策略调用pass策略。

```
[H3C]zone-pair security source Trust
destination Local
[H3C-zone-pair-security-Trust-Local]object-
policy apply ip pass
[H3C-zone-pair-security-Trust-Local]quit
```

#创建Local到Trust域的域间策略调用pass策略。

```
[H3C]zone-pair security source Local
destination Trust
[H3C-zone-pair-security-Local-Trust]object-
policy apply ip pass
[H3C-zone-pair-security-Local-Trust]quit
```

3.3 限制用户SSH登录设备

#只允许内网192.168.10.0/24网段用户登录设备

#配置ACL：

```
[H3C]acl basic 2999
[H3C-acl-ipv4-basic-2999]rule permit source
192.168.10.0 0.0.0.255
[H3C-acl-ipv4-basic-2999]quit
```

#在SSH服务中调用

```
[H3C]SSH server acl 2999
```

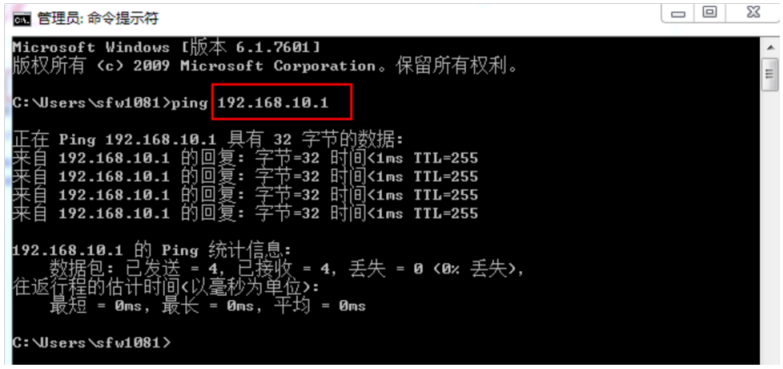
#测试无问题后，再保存配置

```
[H3C]save force
```

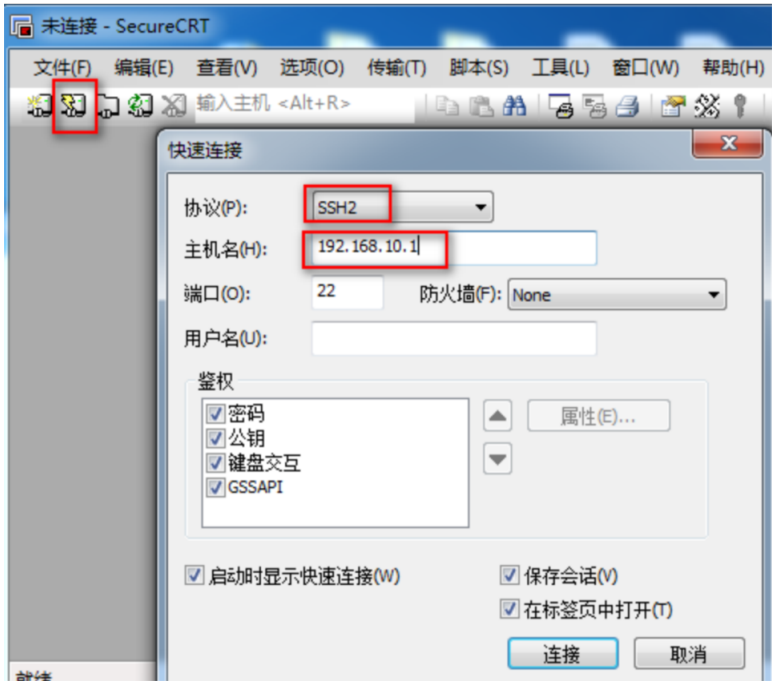
4 配置验证及登录测试

4.1 使用CRT客户端SSH登录设备

#客户端配置地址保证能够ping通防火墙接口地址

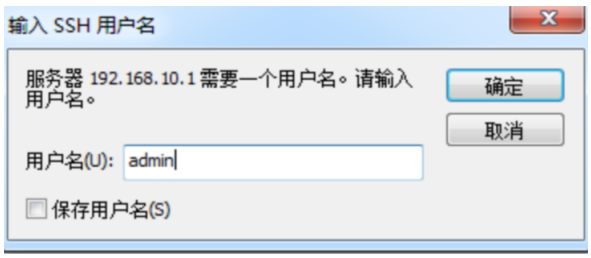


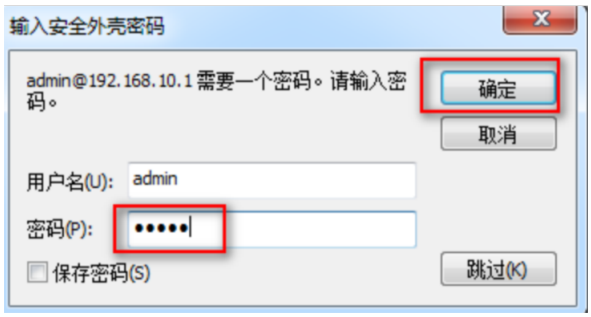
#电脑上开启CRT软件开始连接设备，点击快速连接，然后协议选择"SSH2"，主机名输入设备的地址"192.168.10.1"，点击"连接"。

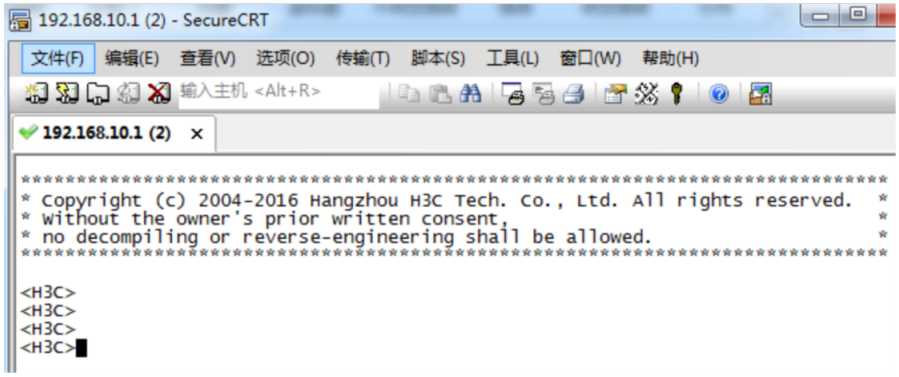


#连接成功后，会跳出新建主机密钥对话框，点击"接受并保存"紧接着就会弹出输入SSH用户名的对话框，输入用户

名“admin”，点击“确定”，然后会接着出来一个对话框，输入密码“admin”，然后点击“确定”后就可以进入设备了。






192.168.10.1 (2) - SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 窗口(W) 帮助(H)
输入主机 <Alt+R>
192.168.10.1 (2)
* Copyright (c) 2004-2016 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
<H3C>
<H3C>
<H3C>
<H3C>