S2000-EA系列交换机充当SSH服务器并采用password远程HWTACACS认证功能的配置

岳斌 2008-11-27 发表

S2000-EA系列交换机充当SSH服务器并采用password远程HWTACACS认证功能的配置

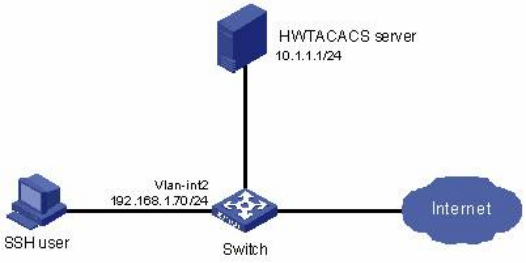
一、 组网需求：

当用户通过一个不能保证安全的网络远程登录到交换机时，为保证数据信息交换的安全性，使用SSH来实现此目的，并采用password远程HWTACACS认证。

（1）PC终端（SSH Client）上运行支持SSH2.0的客户端软件，与交换机（SSH Server）建立本地连接。

（2）配置交换机实现HWTACACS服务器对登录交换机的SSH用户进行认证。

二、 组网图：



三、 配置步骤：

1、 SSH服务器端配置

在交换机上创建VLAN接口，并为其分配IP地址，作为客户端连接的SSH服务器地址。

<Switch> system-view

[Switch] interface vlan-interface 2

[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0

[Switch-Vlan-interface2] quit

生成RSA和DSA密钥对。

[Switch] public-key local create rsa

[Switch] public-key local create dsa

设置用户接口上的认证模式为AAA认证。

[Switch] user-interface vty 0 4

[Switch-ui-vty0-4] authentication-mode scheme

设置用户接口上支持SSH协议。

[Switch-ui-vty0-4] protocol inbound ssh

[Switch-ui-vty0-4] quit

配置HWTACACS方案。

[Switch] hwtacacs scheme hwtac

[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49

[Switch-hwtacacs-hwtac] primary authorization 10.1.1.1 49

[Switch-hwtacacs-hwtac] key authentication expert

[Switch-hwtacacs-hwtac] key authorization expert

[Switch-hwtacacs-hwtac] user-name-format without-domain

[Switch-hwtacacs-hwtac] quit

配置ISP域的AAA方案。

[Switch] domain bbb

[Switch-isp-bbb] scheme hwtacacs-scheme hwtac

指定用户client001的认证方式为password

[Switch] ssh user client001 authentication-type password

2、SSH客户端配置

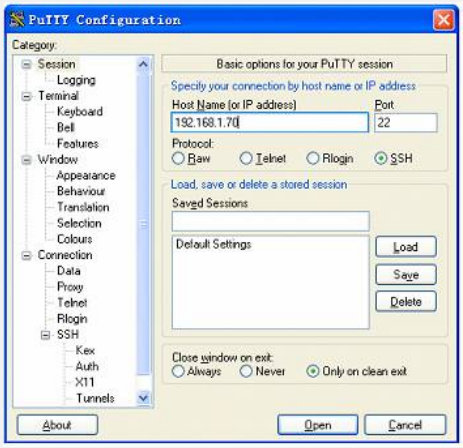
客户端主机配置IP地址

客户端主机的IP地址必须同交换机上的VLAN接口的IP地址位于同一个网段，这里设置为“192.168.1.1”。

建立与SSH服务器端的连接

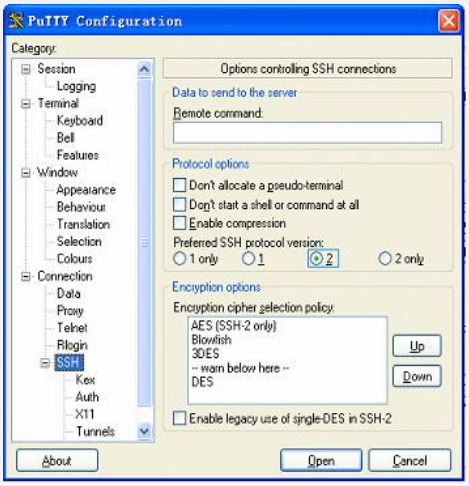
SSH客户端软件的配置（以Putty0.58为例）。

（1）打开PuTTY.exe程序，出现如下客户端配置界面。



在“Host Name（or IP address）”文本框中输入SSH服务器的IP地址。

（2）单击SSH客户端配置界面左边目录树（“Category”）中的连接协议（“Connection”）中的“SSH”，出现下图界面。



在“Protocol options”区域中，选择“Preferred SSH protocol version”参数的值为2。

在上图中，单击<Open>按钮，如果连接正常则会提示用户输入用户名client001及密码。认证成功后，即可登录到服务器端。用户登录系统后所能访问的命令级别由HWTACACS服务器授权，有关服务器授权的配置请参见相关HWTACACS服务器配置手册。

四、 配置关键点：

生成服务器端的RSA和DSA密钥对是完成SSH登录的必要操作。