S2000-EA系列交换机充当SSH服务器并采用公钥认证功能的配置

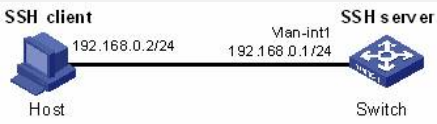
岳斌 2008-11-27 发表

S2000-EA系列交换机充当SSH服务器并采用公钥认证功能的配置

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，为更大限度地保证数据信息交换的安全性，使用SSH来实现此目的，并采用公钥认证。如图1-21所示，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。

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 1

[Switch-Vlan-interface1] ip address 192.168.0.1 255.255.255.0

[Switch-Vlan-interface1] 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

设置用户能访问的命令级别为3。

[Switch-ui-vty0-4] user privilege level 3

[Switch-ui-vty0-4] quit

创建用户client001，并指定认证方式为公钥认证。

[Switch] ssh user client001 authentication-type publickey

在服务器端从文件public中导入客户端的公钥，公钥名为Switch001。

[Switch] public-key peer Switch001 import sshkey public

为用户client001指定公钥Switch001。

[Switch] ssh user client001 assign publickey Switch001

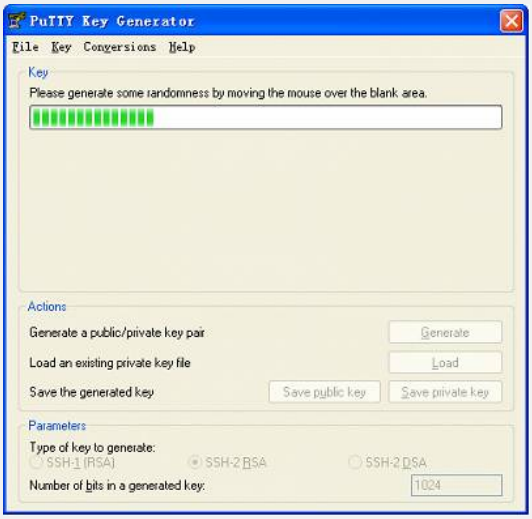
2、SSH客户端的配置（以Putty0.58为例）。

生成密钥对。

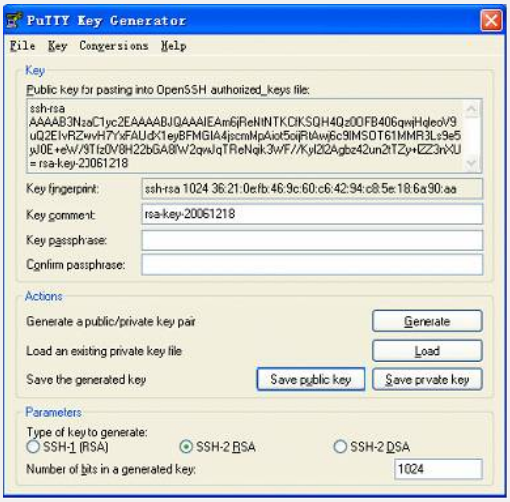
运行PuTTYGen.exe，选择要生成的密钥对。此处参数栏选择“SSH2(RSA)”，点击<Generate>，产生客户端密钥对。

在产生密钥对的过程中需不停的移动鼠标，鼠标移动仅限于下图蓝色框中除绿色标记

进程条外的地方，否则进程条的显示会不动，密钥对将停止产生。



密钥对产生后，点击<save public key>，输入存储公钥的文件名public，点击保存。

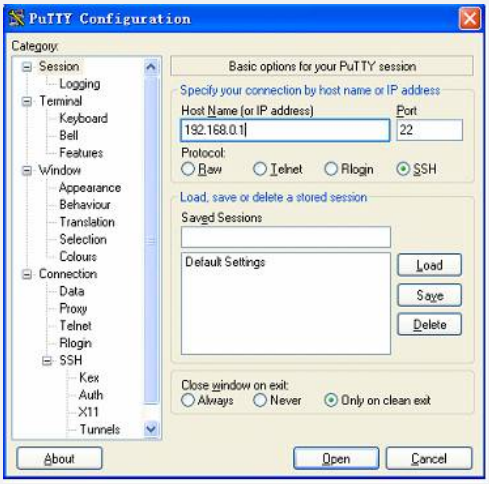


同理，点击<save private key>存储私钥，弹出警告框，提醒是否保存没做任何保护措施的私钥，点击<Yes>，输入私钥文件名即可，此处为private.ppk，点击保存。

客户端生成密钥对后，需要将保存的公钥文件通过FTP/TFTP方式上传到服务器端，并完成服务器端配置后，才可继续客户端的配置。

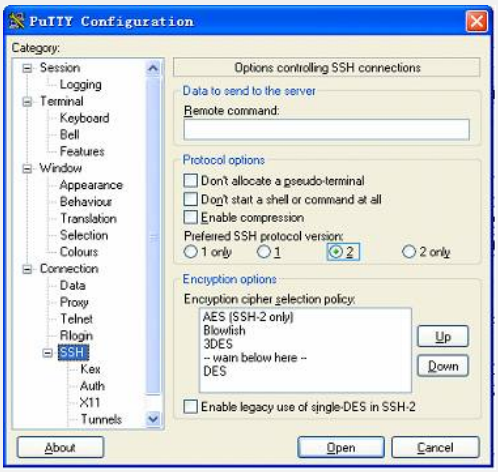
建立与SSH服务器端的连接

（1）打开PuTTY.exe程序，出现下图所示的客户端配置界面。



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”，出现如图1-27的界面。



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

（3）单击“SSH”下面的“Auth”（认证），出现如下图界面。

单击<Browse…>按钮，弹出文件选择窗口。选择与配置到服务器端的公钥对应的私钥文件，并确定即可。

如上图，单击<Open>按钮，如果连接正常则会提示用户输入用户名client001。认证成功后，即可登录到服务器端。

四、 配置关键点：

（1）采用公钥认证时，可以采用RSA或DSA公钥作为服务器端认证客户端的公钥。这里以RSA公钥为例。

（2）生成服务器端的RSA和DSA密钥对是完成SSH登录的必要操作。