堡垒机操作指南

1、堡垒机系统功能指南

1.1 用户登录及密码修改

用户在浏览器输入地址 https://sas.scau.edu.cn，输入现教中心分配的堡垒机账号和密码，点击登录。

初始登录必须修改密码。进入系统后也可在页面的右上角进行“修改密码”。

1.2 工具下载

提供了运维工具及 web 访问设备的所需的插件，用户可通过“运维管理”—“工具下载”，下载所需的工具或插件。

1.3 使用说明

堡垒机提供多种访问设备的方式，包括 SSH、RDP、TELNET、VNC、FTP、SFTP 等。建议设备为 windows 系统的采用 RDP 方式，设备为 linux 系统的采用 SSH/SFTP 方式。以下分别介绍 RDP,SSH/SFTP,WEB 三种方式访问设备的步骤。

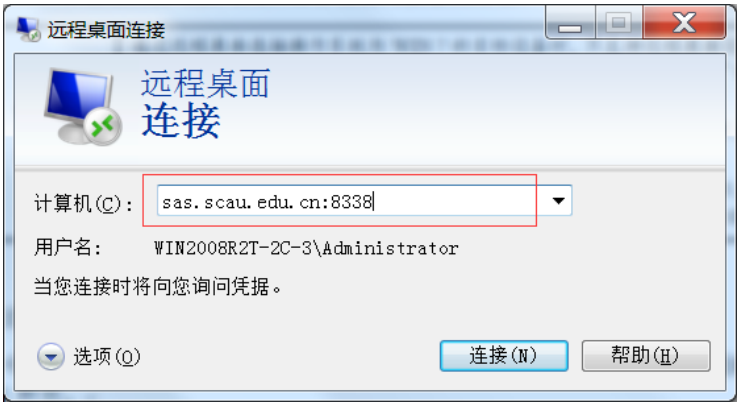
2、通过 RDP 第三方工具访问设备

以 Windows 远程桌面连接为例介绍访问设备的方法。

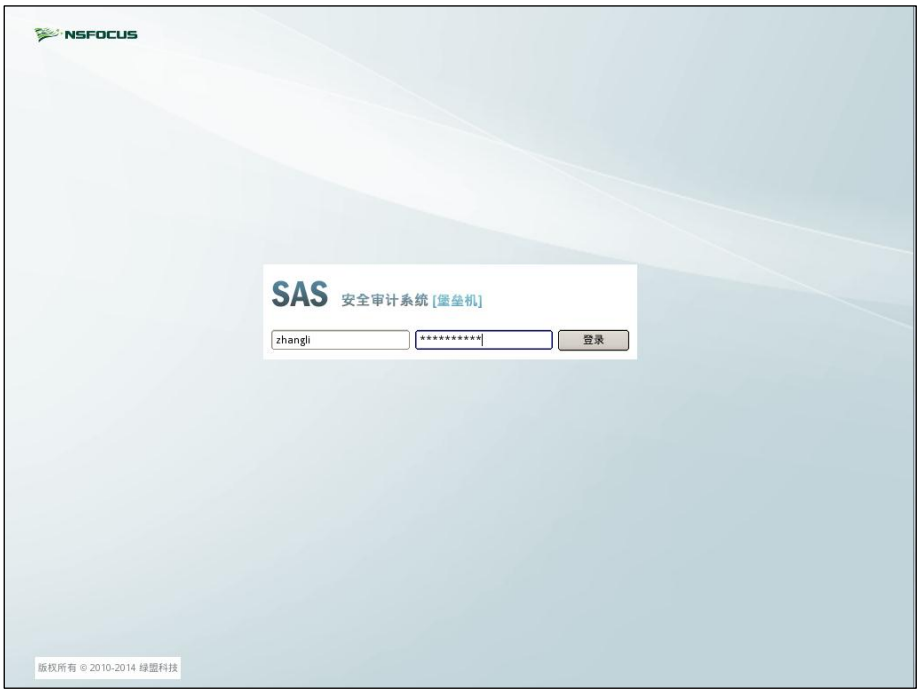
说明	通过远程桌面连接操作系统为 WIN 7 的目标设备时，不支持远程桌面设置为“仅允许运行使用网络级别身份验证的远程桌面的计算机连接（更安全）”的目标设备； 通过远程桌面连接操作系统为 Windows Server 2003 的目标设备时，不支持终端服务配置中加密级别设置为“符合 FIPS 标准”的目标设备； 通过远程桌面连接操作系统为 Windows Server 2008 的目标设备时，不支持终端服务配置中加密级别设置为“符合 FIPS 标准”或“SSL (TLS 1.0)”的目标设备。

通过远程桌面连接访问设备的步骤如下：

步骤 1：在命令行输入 mstsc 或者单击**开始>所有程序>附件>远程桌面连接**，运行远程桌面连接工具。



步骤 2：在步骤 1 中，输入远程登录的堡垒机的 IP 地址后，单击【连接】，进入登录堡垒机界面。



步骤 3：在步骤 2 中输入堡垒机用户的用户名和密码，单击【登录】，进入登录目标设备界面。如勾选“记住密码”，下次登陆即可直接进入设备系统界面。


sas.scau.edu.cn:8338 - 远程桌面连接
NSFOCUS
选择设备
分组方式：
设备类型
设备类型：
WINDOWS服务器
设备名称：
设备IP：
192.168.
访问协议：
RDP
设备账号：
设备密码：
记住密码
Console模式：
禁用
启用
登录
版权所有 © 2010-2016 绿盟科技

3、通过 SSH、SFTP 第三方工具访问设备

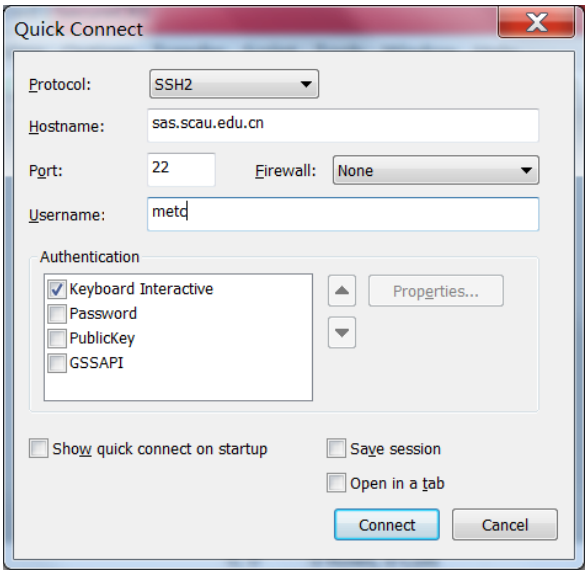
3.1 SSH 工具访问设备

以 SecureCRT 工具为例，通过 SSH 第三方工具访问设备的方法。

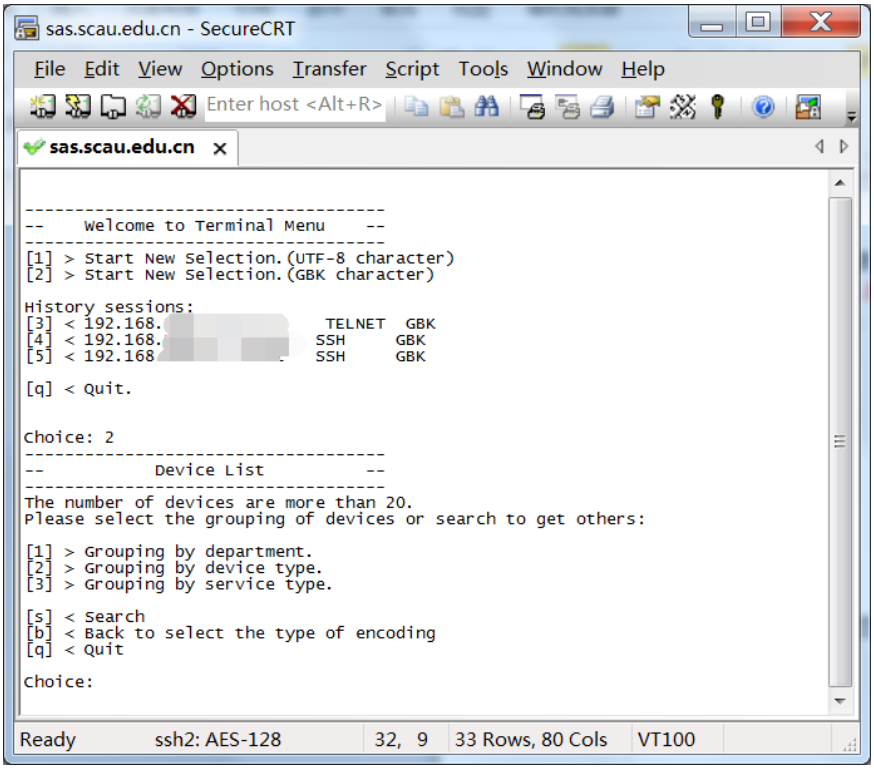
通过 SecureCRT 工具访问设备的步骤如下：

步骤 1：打开 SecureCRT 工具，配置快速连接信息。

Protocol（协议）为 **ssh2**，Port(端口)默认为 22，Hostname（堡垒机的 IP 地址）为 **sas.scau.edu.cn**，Authentication（认证类型）为 **Kerboard Interact**，Username（用户名）为**分配的账号**。



步骤 2：在步骤 1 中单击【Connect】，并输入**堡垒机的登陆密码**。进入连接设备界面。**选择编码**之后，再选择要访问的设备 IP 地址和访问协议。



步骤 3：登录设备。输入登录设备的用户名和密码，即可成功登录设备。

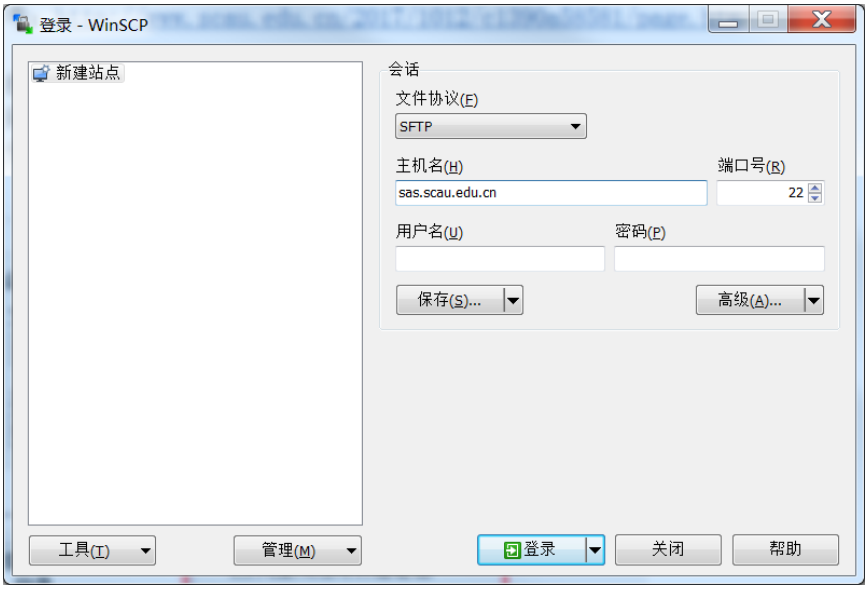
3.2 SFTP 工具访问设备

以 Winscp 工具为例，通过 SFTP 第三方工具访问设备的方法。

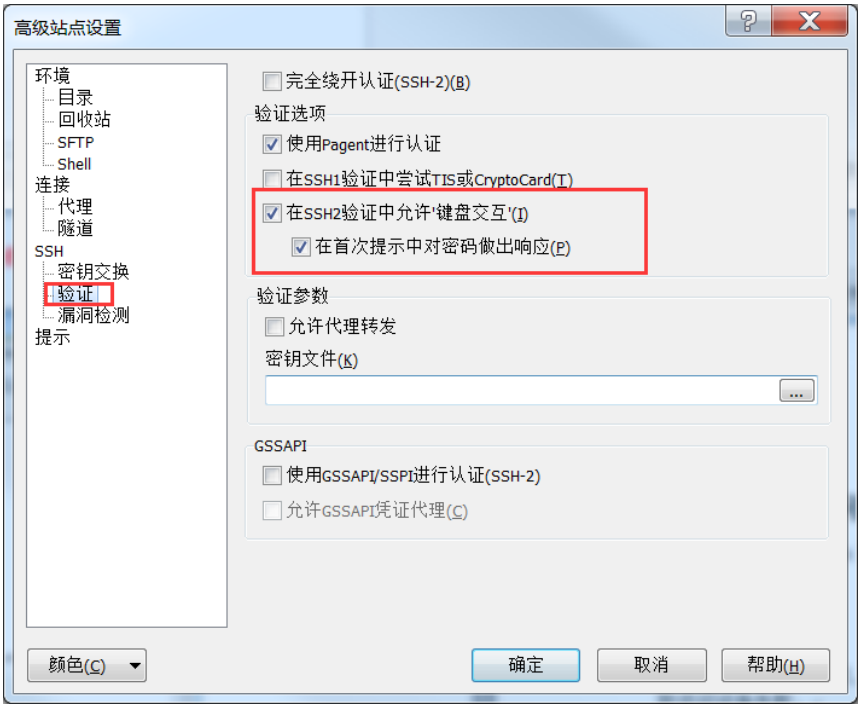
通过 Winscp 工具访问设备的步骤如下：

步骤 1：打开 Winscp 工具，新建站点。

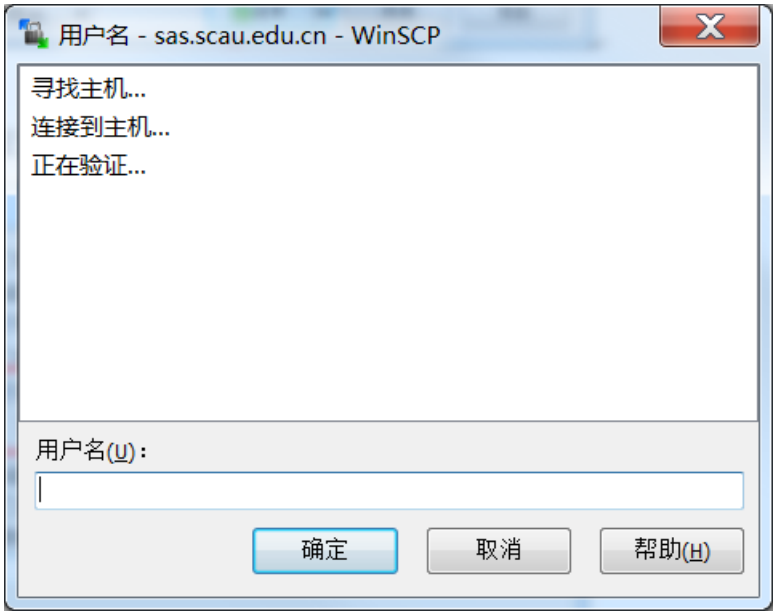
Protocol（协议）为 **SFTP**， Port(端口号)为 22， Hostname（主机名）为 **sas.scau.edu.cn**。

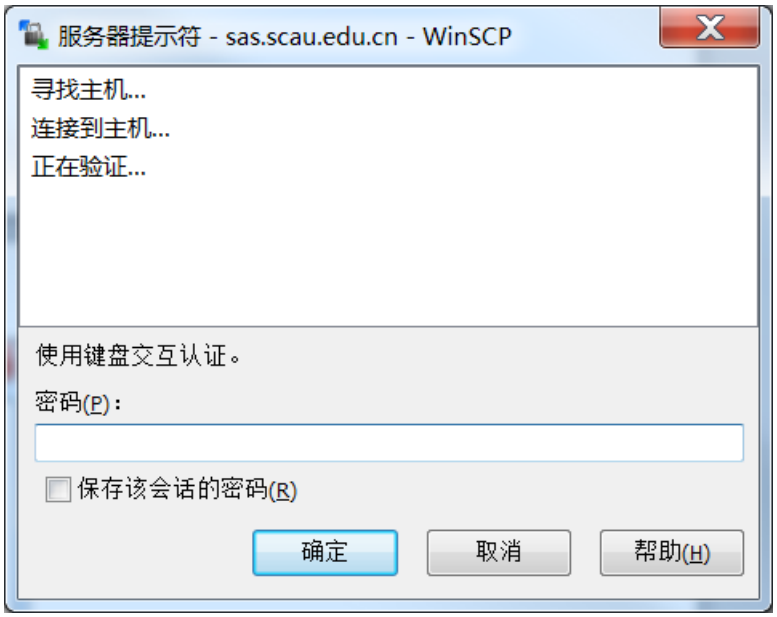


确认高级选项中的验证方式为 Kerboard Interact（键盘交互）。

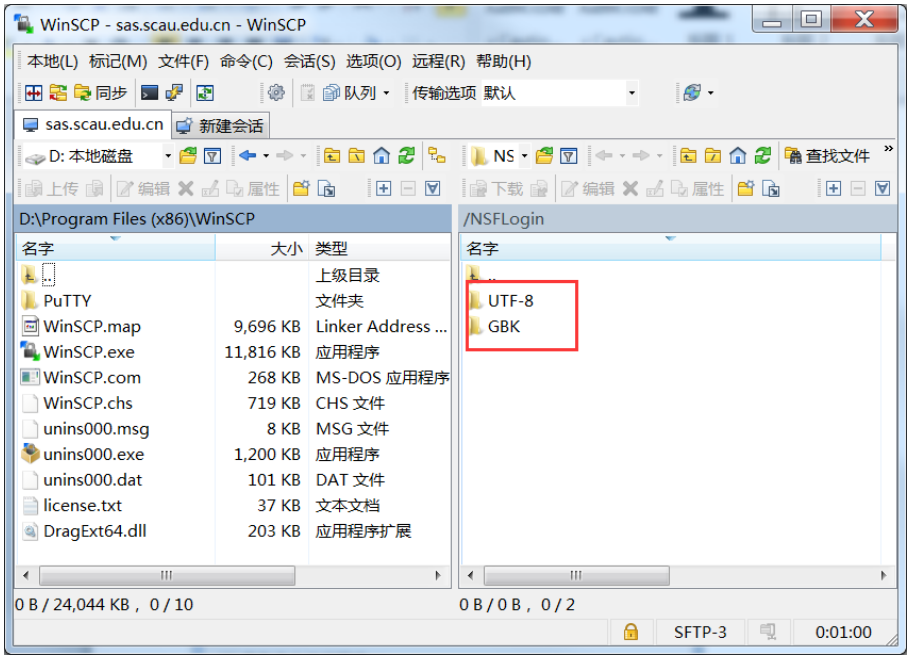


步骤 2：输入现教中心分配的堡垒机账号及对应的密码。

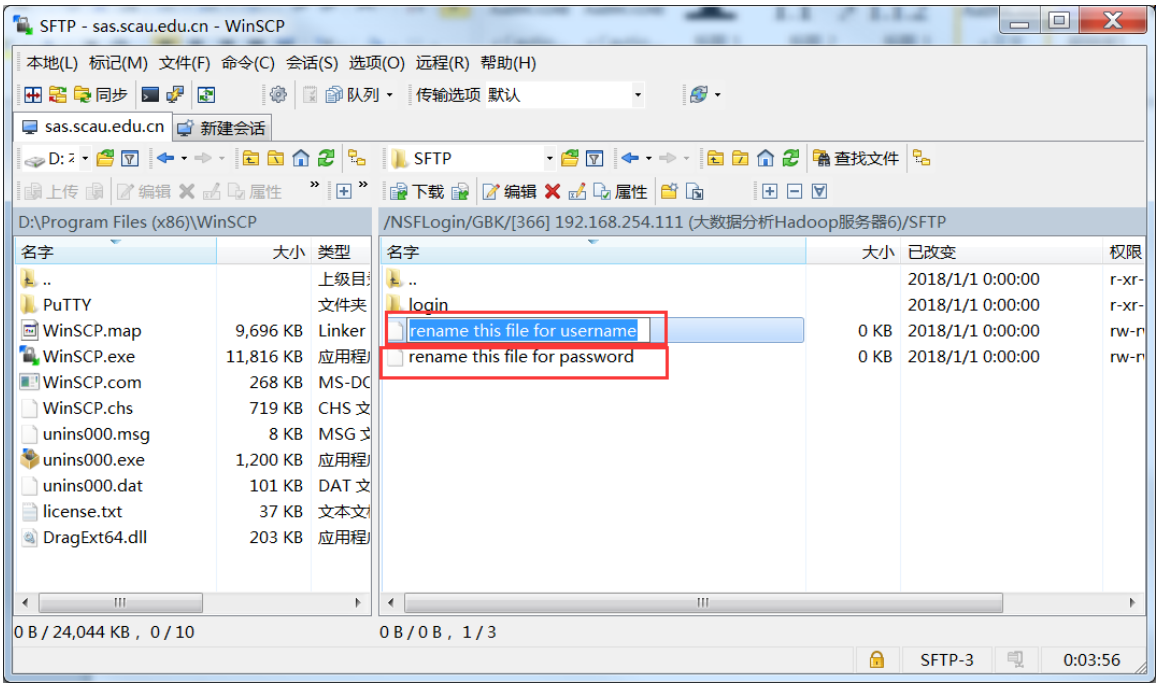




步骤 3：选择相应的显示编码方式后，选择要登陆的服务器。



步骤 4：重命名下图的两个文件的名称，username 为服务器**操作系统的管理员账号**，password 为该管理员账号对应的密码。之后点击“login”即可访问设备资源。



4、通过 Web 页面访问设备

系统支持用户通过 Web 页面方式访问设备，但需要做较多的设置，务必按照指引进行配置。

4.1 安装 JAVA 虚拟机

通过堡垒机访问设备前，必须在客户端安装 JAVA 虚拟机（推荐使用 JAVA1.8.0_29 版本），否则可能导致访问设备失败。

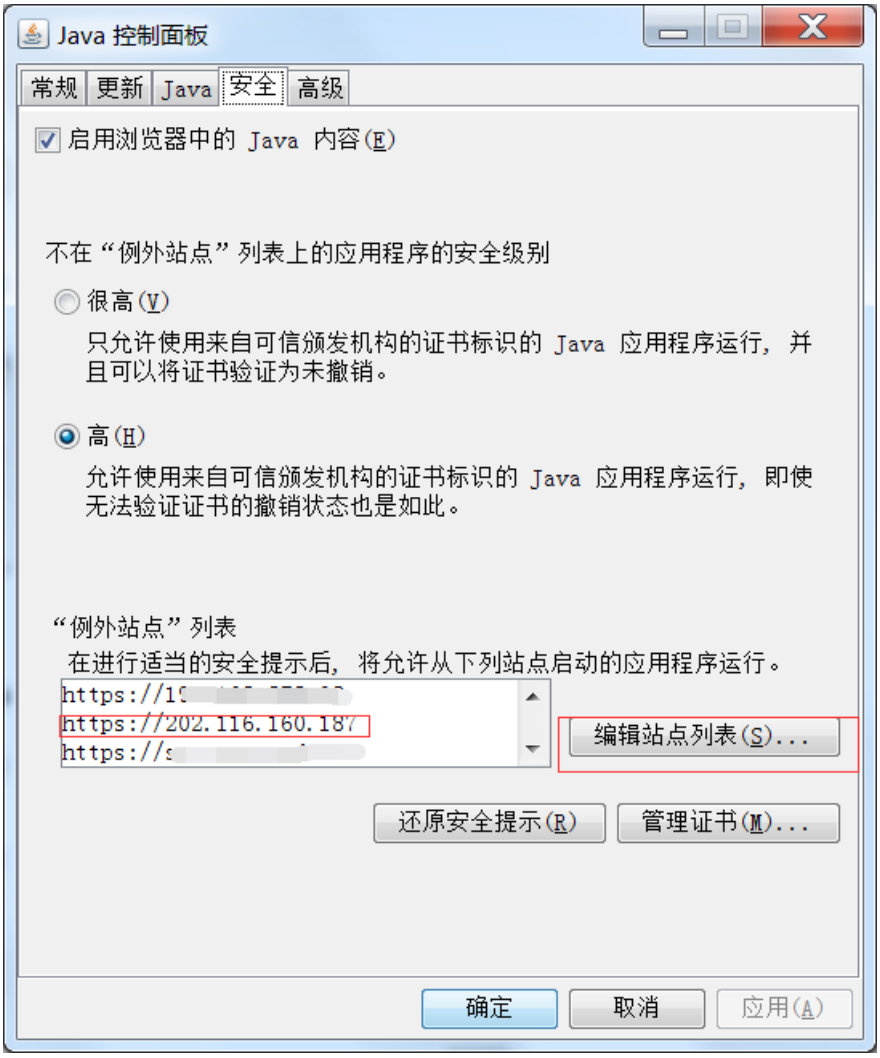
成功安装 JAVA 虚拟机后，还需要设置 jre 安全设置和修改浏览器安全设置。

4.2 jre 安全设置

以 WINDOWS 操作系统为例，设置 jre 安全设置的具体操作如下：

步骤 1：鼠标右键选择“控制面板”，在控制面板下选择“Java”，打开 Java 控制面板。

步骤 2：在 Java 控制面板中选择“安全”选项，并在例外站点列表中添加堡垒机 IP 地址 **https://202.116.160.187**。

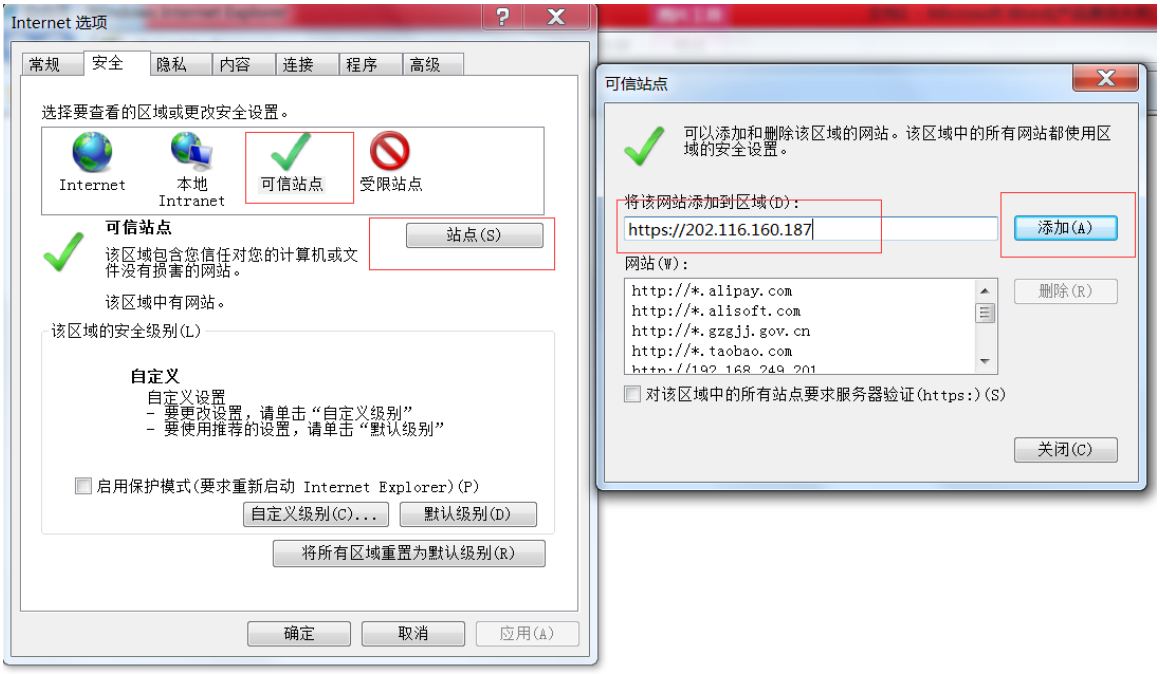


4.3 浏览器安全设置

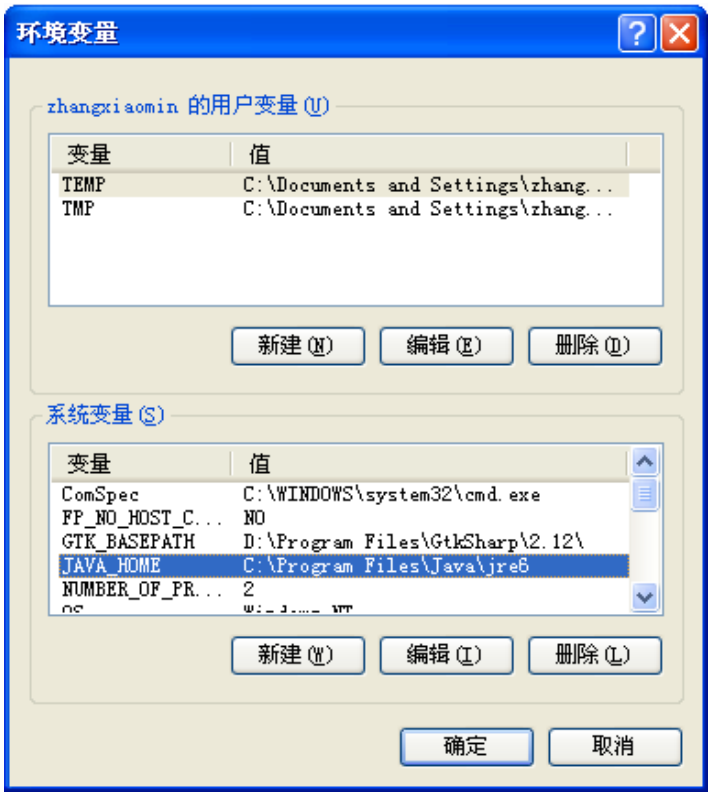
以 WINDOWS 操作系统下的 IE 浏览器为例，设置浏览器安全设置的具体操作如下：

步骤 1：打开 IE 浏览器的“Internet 选项”配置，选择“安全”选项卡。

步骤 2：选择“受信任的站点”，并在“站点”配置中添加堡垒机 URL 地址 **https://202.116.160.187**。



建议修改 JAVA 的环境变量，否则某些客户端无法通过堡垒机访问设备。以 WINDOWS 操作系统为例，修改方法为：鼠标右键选择“我的电脑>属性>高级”，单击【环境变量】，进入环境变量页面。在环境变量页面新建一个名称为 **JAVA_HOME**、值为 **jre** 或 java 安装目录（如 C:\Program Files\Java\jre6）的系统环境变量。



4.4 登录设备

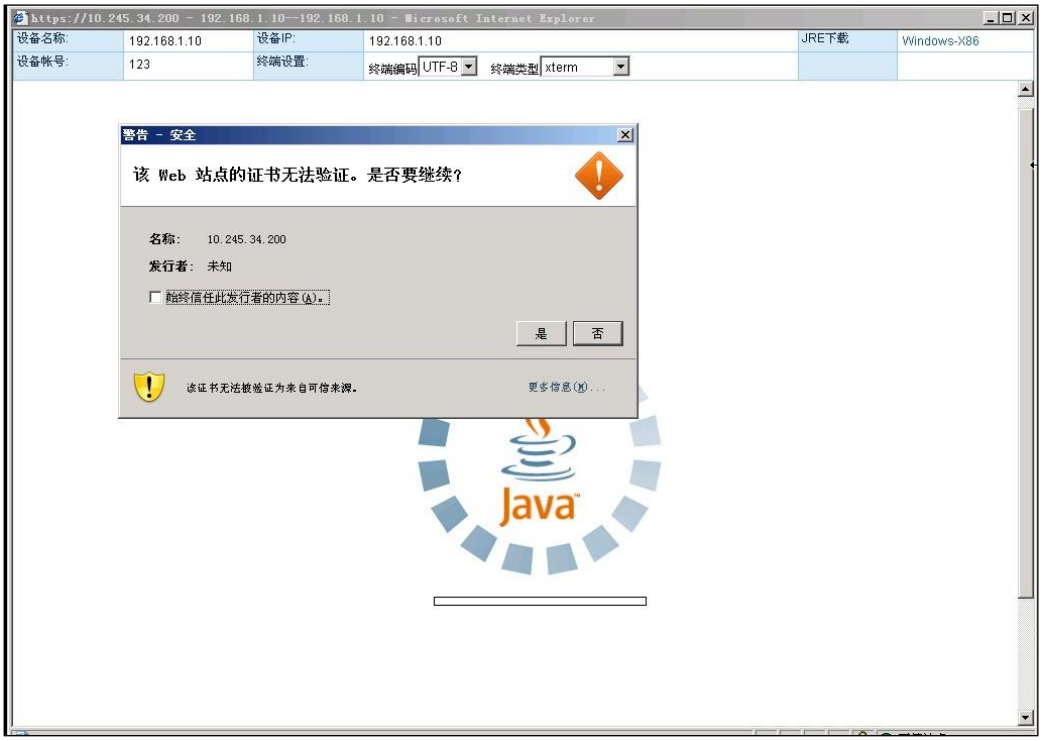
访问设备的步骤如下：

步骤 1：在设备访问页面，点击“切换至原模式”选择要访问的设备和访问类型。

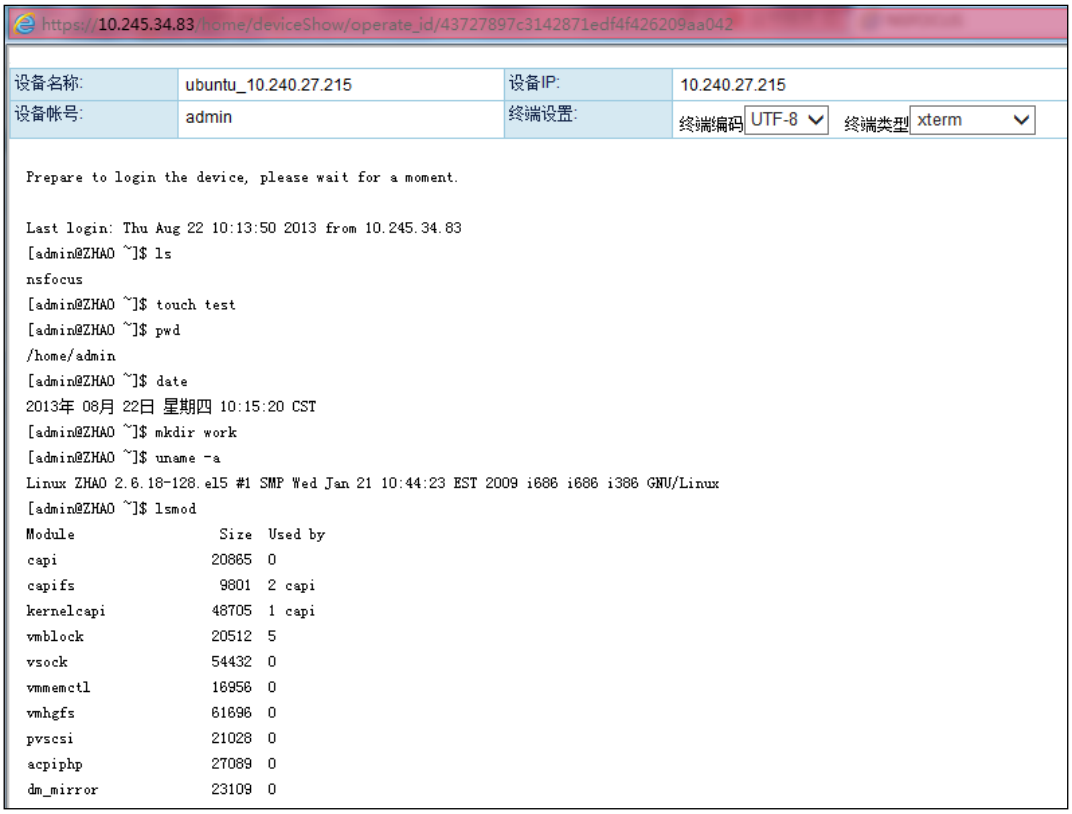
此处选择 UNIX/LINUX 服务器类型下名为**内网服务器**的服务器，并在**内网服务器**下选择登录使用的协议**SSH**。

步骤 2：选择 SSH 协议。在步骤 1 中单击链接 **SSH**，进入设备账号选择界面。

步骤 3：（可选）：选择设备账号。在步骤 2 中单击链接 **admin**，弹出安全警告。



步骤 4：在步骤 3 中勾选**始终信任此发行者的内容**，并单击【是】，成功进入访问设备页面。


https://10.245.34.83/home/deviceShow/operate_id/43727897c3142871edf4f426209aa042
设备名称:
ubuntu_10.240.27.215
设备IP:
10.240.27.215
设备帐号:
admin
终端设置:
终端编码 UTF-8
终端类型 xterm
Prepare to login the device, please wait for a moment.
Last login: Thu Aug 22 10:13:50 2013 from 10.245.34.83
[admin@ZHAO ~]$ ls
nsfocus
[admin@ZHAO ~]$ touch test
[admin@ZHAO ~]$ pwd
/home/admin
[admin@ZHAO ~]$ date
2013年 08月 22日 星期四 10:15:20 CST
[admin@ZHAO ~]$ mkdir work
[admin@ZHAO ~]$ uname -a
Linux ZHAO 2.6.18-128.el5 #1 SMP Wed Jan 21 10:44:23 EST 2009 i686 i686 i386 GNU/Linux
[admin@ZHAO ~]$ lsmod
Module Size Used by
capi 20865 0
capifs 9801 2 capi
kernelcapi 48705 1 capi
vmblock 20512 5
vsock 54432 0
vmmemctl 10958 0
vmhgfs 61696 0
pvscsi 21028 0
acpiphp 27089 0
dm_mirror 23109 0