F1000-X-G2/F100-X-G2系列V7防火墙使用默认证书配置SSL VPN IP资源典型案例

SSL VPN　zhiliao_FO3qD　2018-11-25 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

本案例适用于如F1000-A-G2、F1000-S-G2、F100-M-G2、F100-S-G2等F1000-X-G2、F100-X-G2系列的防火墙。

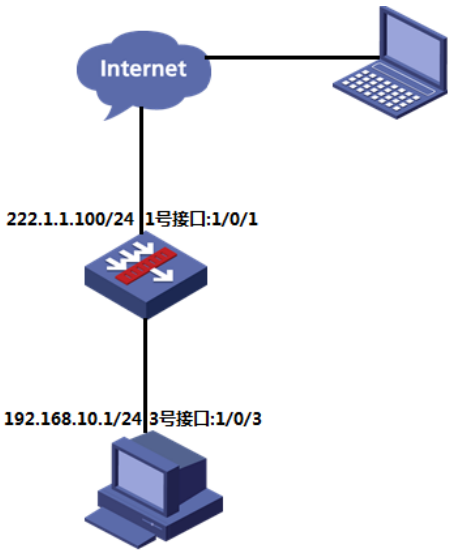
注：本案例是在F1000-C-G2的Version 7.1.064, Release 9323P19版本上进行配置和验证的。

1.2 配置需求及实现的效果

V7防火墙设备作为出口设备，外网PC通过inode软件拨SSLVPN，认证成功后可以访问内网192.168.10.0网段的资源。IP地址及接口规划如下表所示：

外网接口	公网地址/掩码	内网接口	内网地址/掩码
GE1/0/1	222.1.1.100/24	GE1/0/3	192.168.10.1/24

2 组网图



配置步骤

3 配置步骤

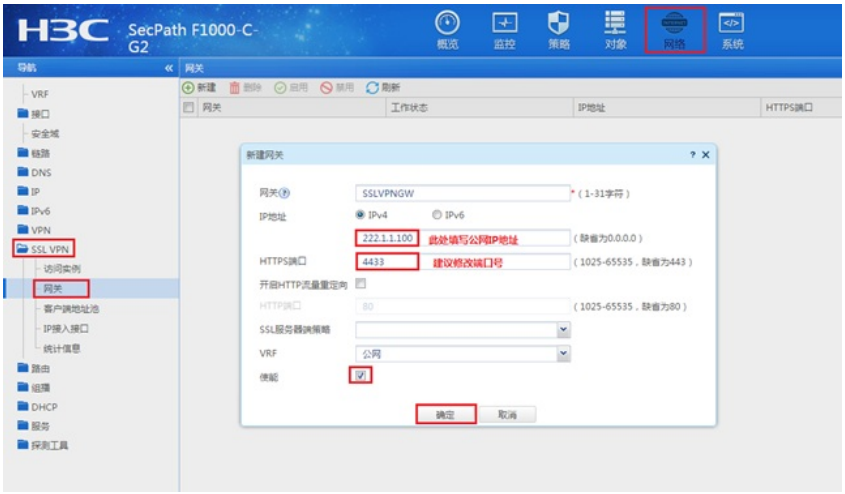
3.1 防火墙上网配置

防火墙上网配置请参考“2.2.2 防火墙外网使用固定IP地址上网配置方法”进行配置，本文只针对SSLVPN配置进行介绍。

3.2 配置SSL VPN网关

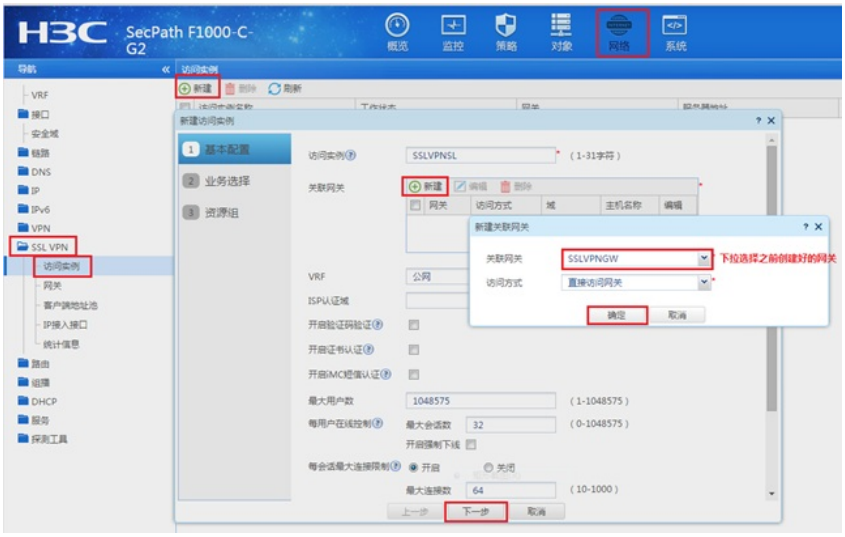
#选择 “网络”>“SSL VPN”>“网关”点击”新建”，IP地址填写防火墙1口地址222.1.1.1.00，端口号修改为4433，缺省端口为443，443端口和https端口冲突。勾选“使能”选项点击“确认”

完成配置

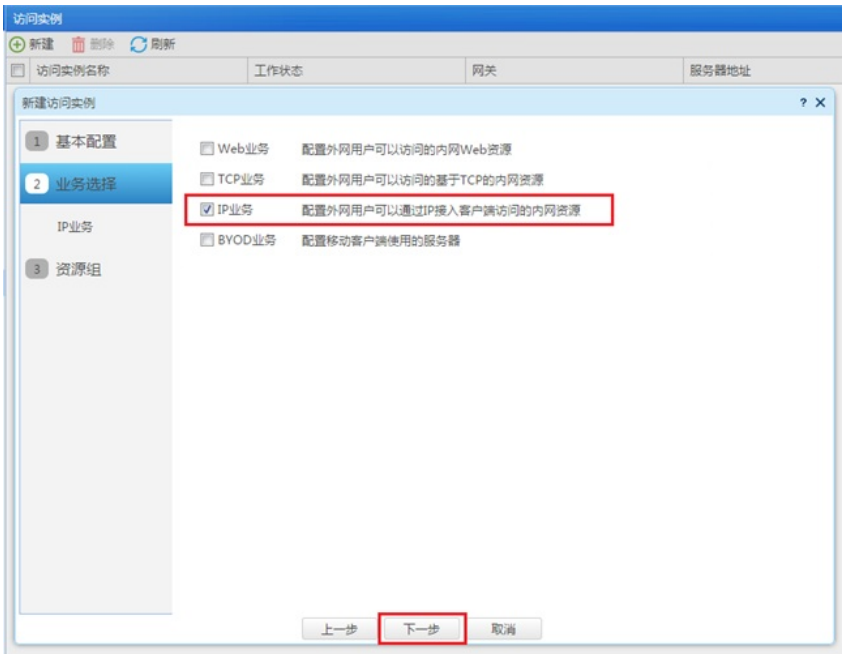


3.3 配置SSL VPN实例

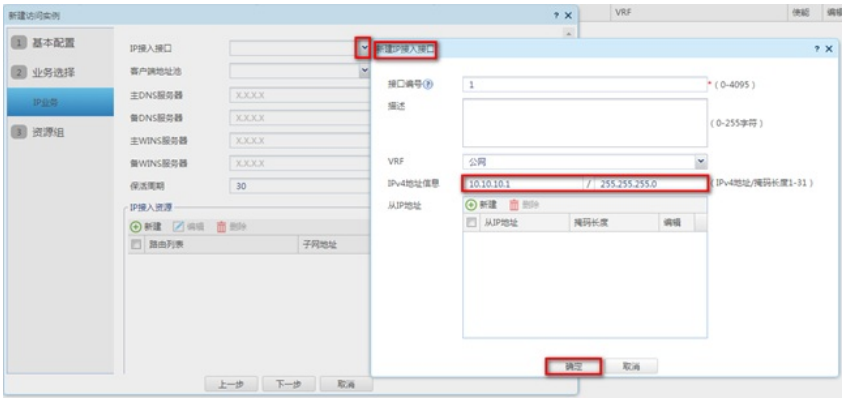
#选择 “网络”>“SSL VPN”>“访问实例”中点击新，在“关联网关”中点击新建，下拉选择上一步创建的SSL VPN网关，确定后点击“下一步”



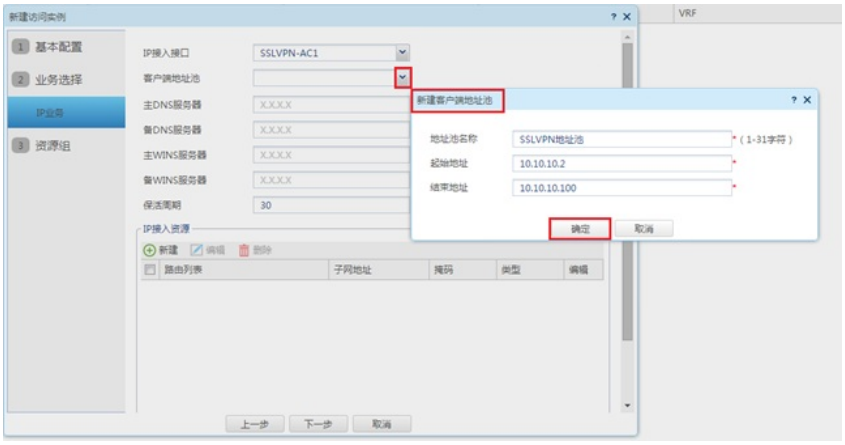
#勾选“IP业务”，然后点击“下一步”



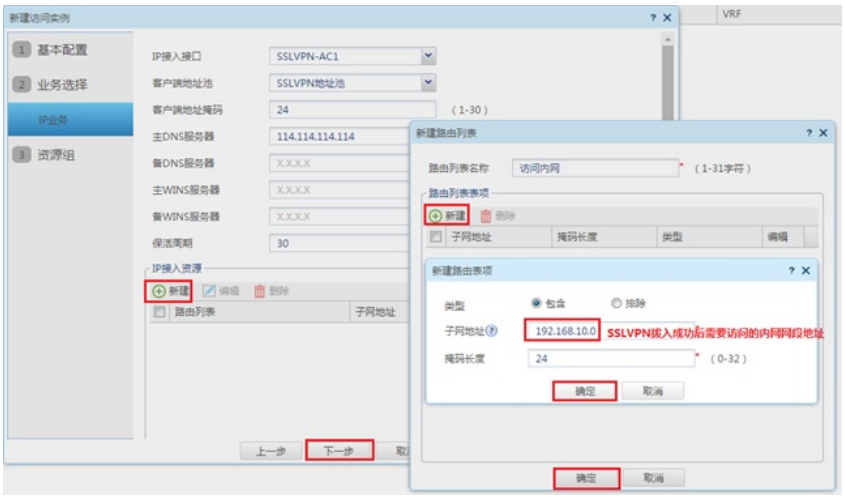
#新建SSL VPN接口，接口编号为1，配置SSL VPN接口IP，IP地址不要和内网网段冲突，配置完成点击“确定”。



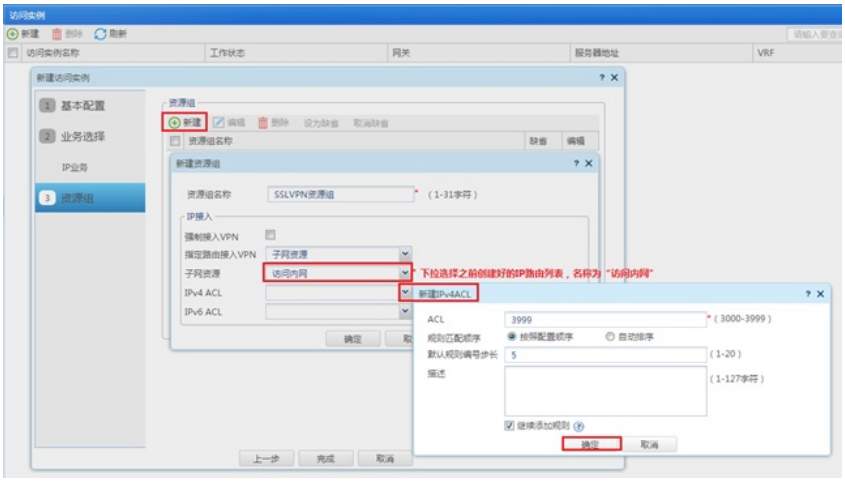
#新建SSL VPN客户端地址池，用于给认证成功后的SSL VPN终端下发地址



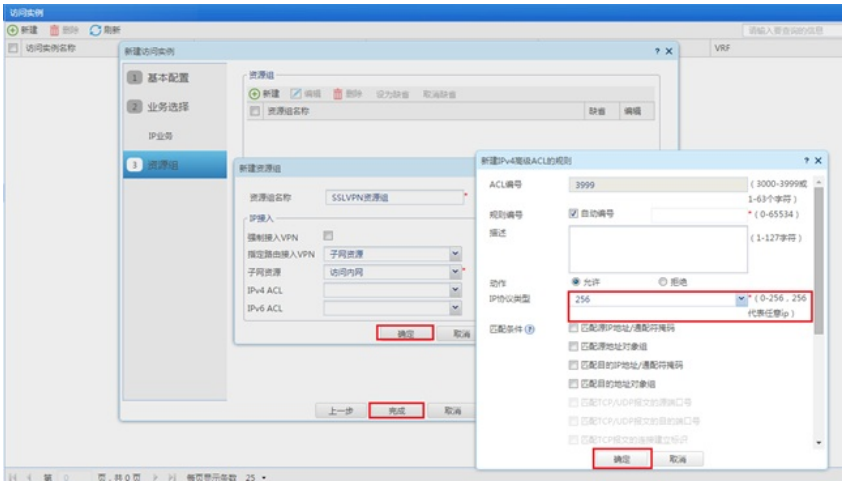
#填写客户端地址掩码，主dns服务器地址（可选），在“IP接入资源”中新建路由列表，列表名称为“访问内网”，路由列表中添加SSL VPN认证成功后需要访问的内网网段地址，确定后点击“下一步”



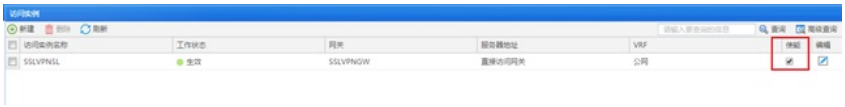
#新建资源组，组名称为“SSLVPN”资源组，指定路由接入VPN中选择“子网资源”，子网资源引用之前创建的IP路由列表“访问内网”，新建IPV4 ACL 3999，只有通过ACL检查的报文才可以访问IP资源



#IPV4 ACL 3999中IP协议类型中填写256，256代表任意IP,配置完IPV4 ACL 3999点击“确定”，再点击“完成”

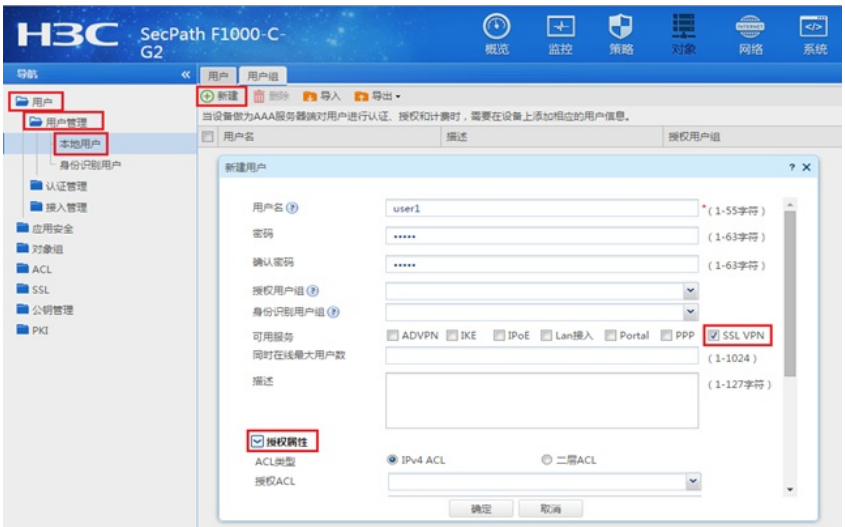


#实例配置完成后勾选“使能”选项来生效配置

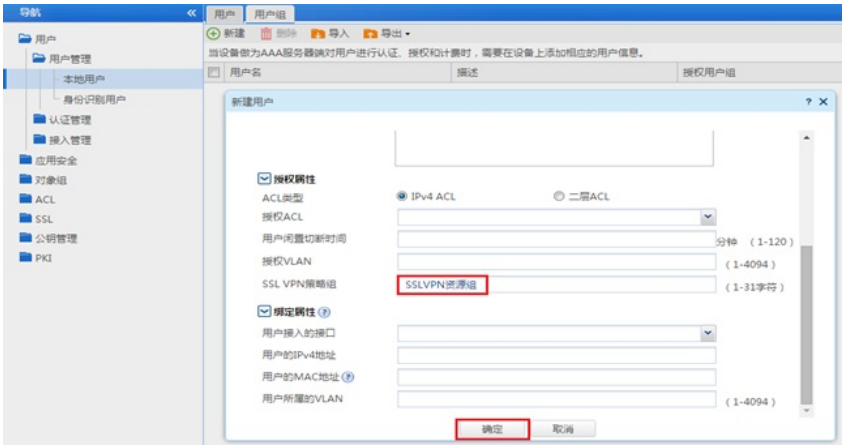


3.4 新建SSL VPN拨号用户，关联SSL VPN策略组

#选择 “对象”>“用户”>“用户管理”>“本地用户”点击“新建”， 来新建SSLVPN用户，配置用户名密码，可用服务中选中SSL VPN

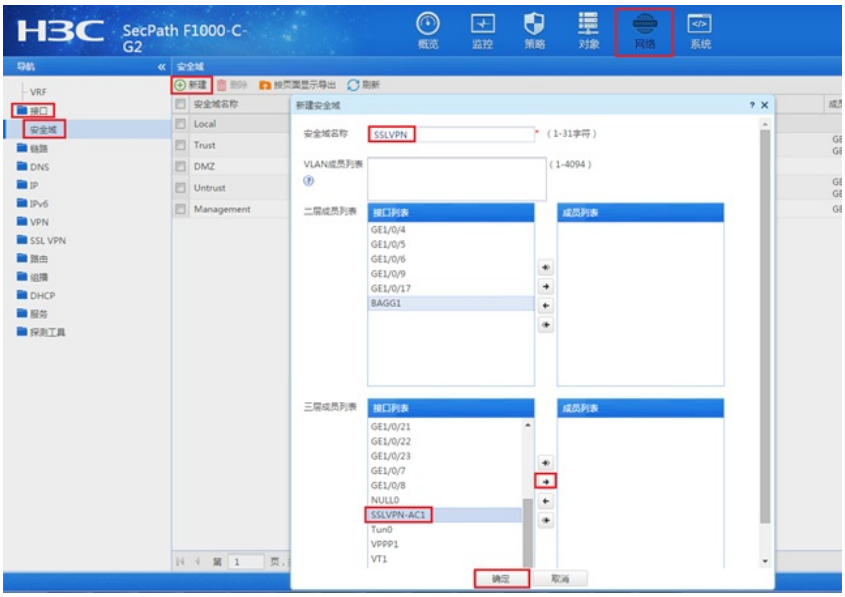


#点击“授权属性”>“SSL VPN策略组”填写SSL VPN实例中创建的SSLVPN资源组，点击“确定”完成配置

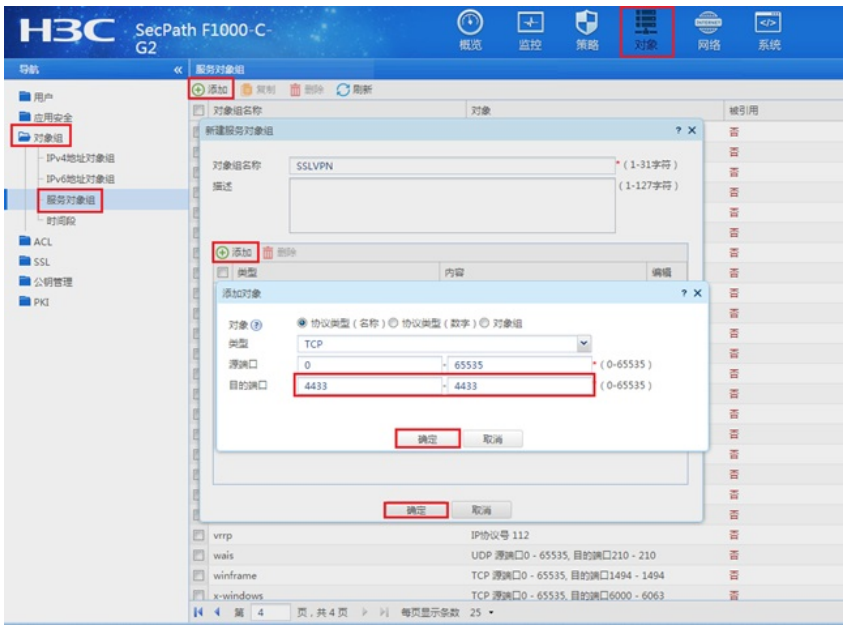


3.5 将SSL VPN端口加入安全域，放通对应安全策略

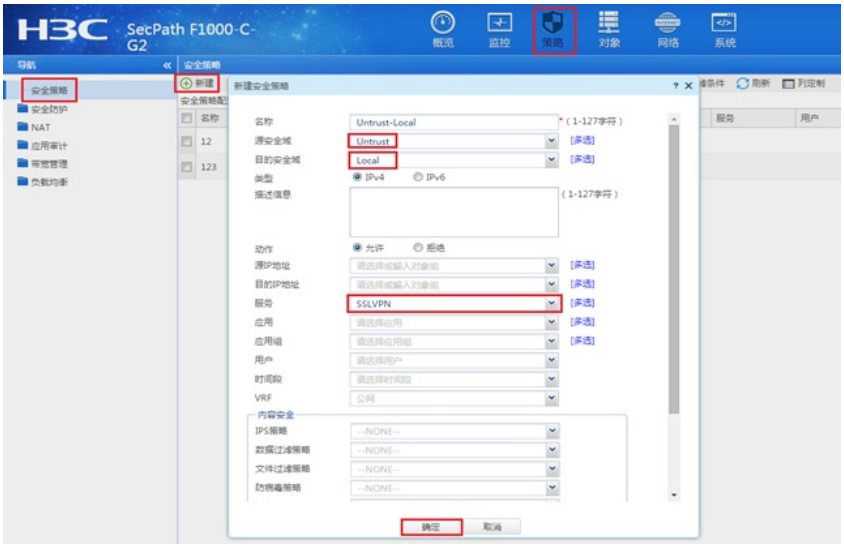
#选择“网络”>“接口”>“安全域”点击新建，安全域名称为“SSLVPN”,三层成员列表中选中SSLVPN-AC1接口加入到此安全域



#选择“对象”>“对象组>“服务对象组”点击“添加”，对象组名称“SSLVPN”,添加对象，类型为TCP,目的端口为SSL VPN端口4433



#选择“策略”>“安全策略”>点击新建，策略名称为“Untrust-Local”,源安全域为Untrust,目的安全域为Local,服务引用之前创建好的服务对象“SSLVPN”

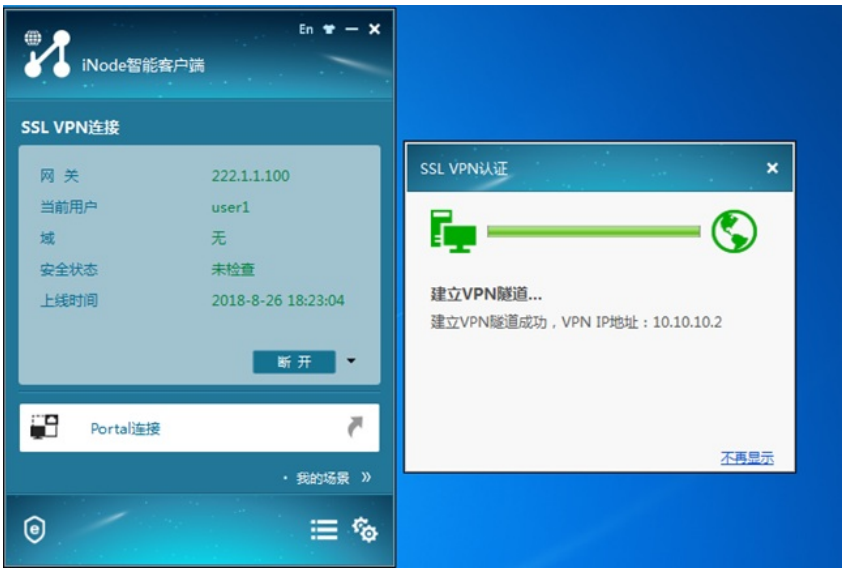


#新建安全策略，策略名称为“SSLVPN-Trust,源安全域为SSLVPN,目的安全域为Trust

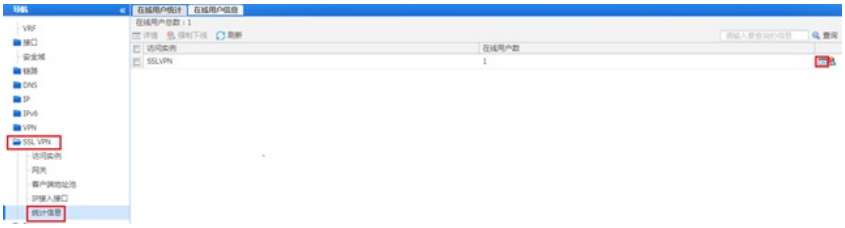
3.6 配置验证，查看拨号成功的用户

#输入SSLVPN网关地址加端口，输入用户名密码点击连接

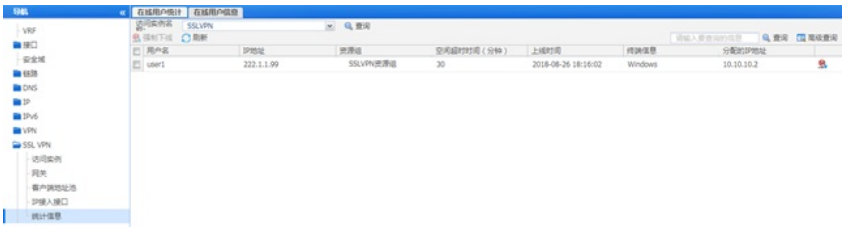
拨号成功后获取到SSLVPN地址池中IP地址



#在“网络”>“SSL VPN”>“统计信息”>中查看拨入成功的用户

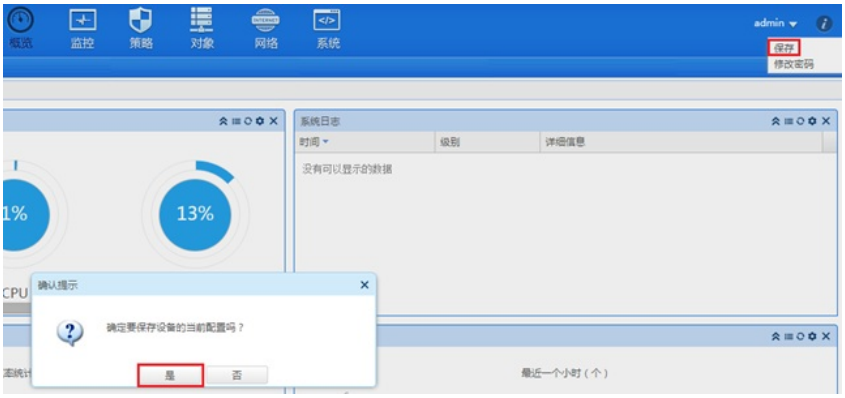


#点击详细可以查看终端详细信息，如：拨号的用户名，分配到的IP地址等



3.7 保存配置

#在设备右上角选择“保存”选项，点击“是”完成配置。



4 注意事项

1、本案例适应的是默认证书，不需要手工导入CA证书和本地正常

2、不需要配置SSL服务器端策略，SSLVPN网关不需要引用SSL服务器端策略

配置关键点