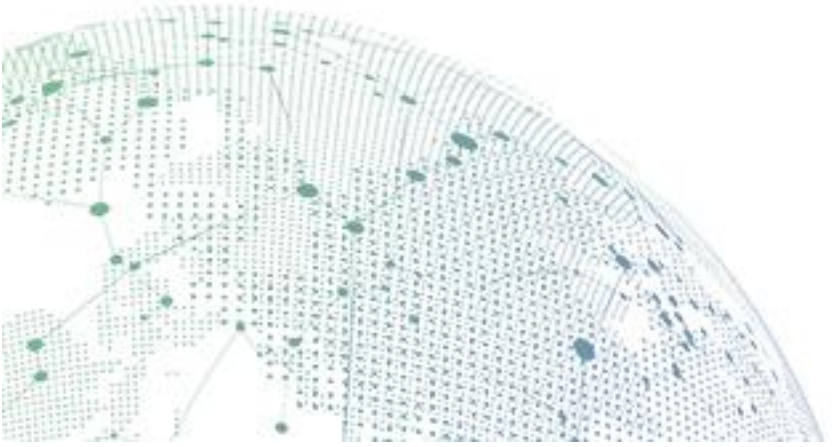
SANGFOR

NGAF

SSL VPN Configuration Guide

Version 8.0.5



Change Log

Date	Change Description

CONTENT

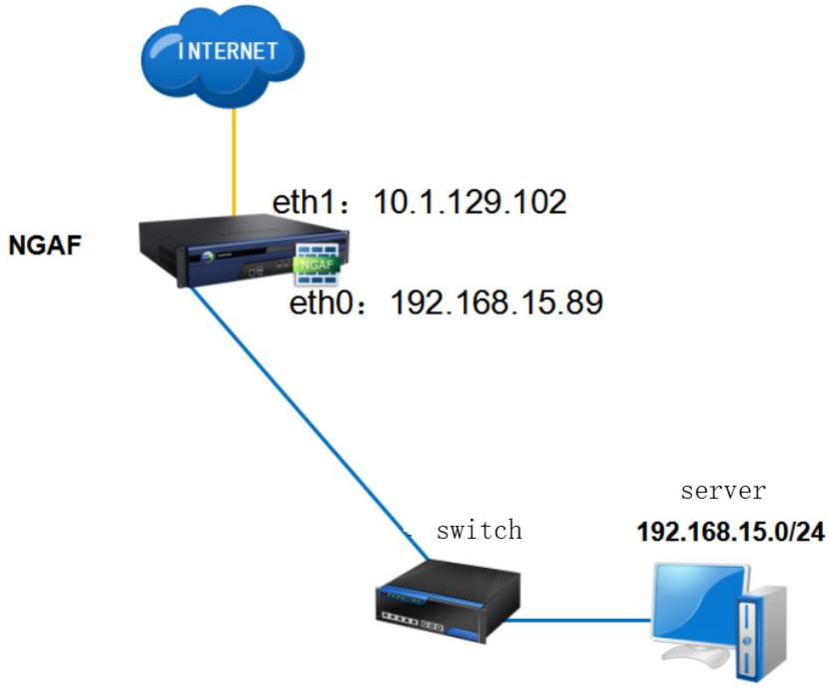
Chapter 1 SSLVPN Function Describe

The role of SSL VPN is to facilitate mobile office users or branch users to access intranet resources of the company's internal intranet through SSL VPN anytime and anywhere and also realize data encryption to ensure data integrity, confidentiality and reliability.

Chapter 2 Application Scenario

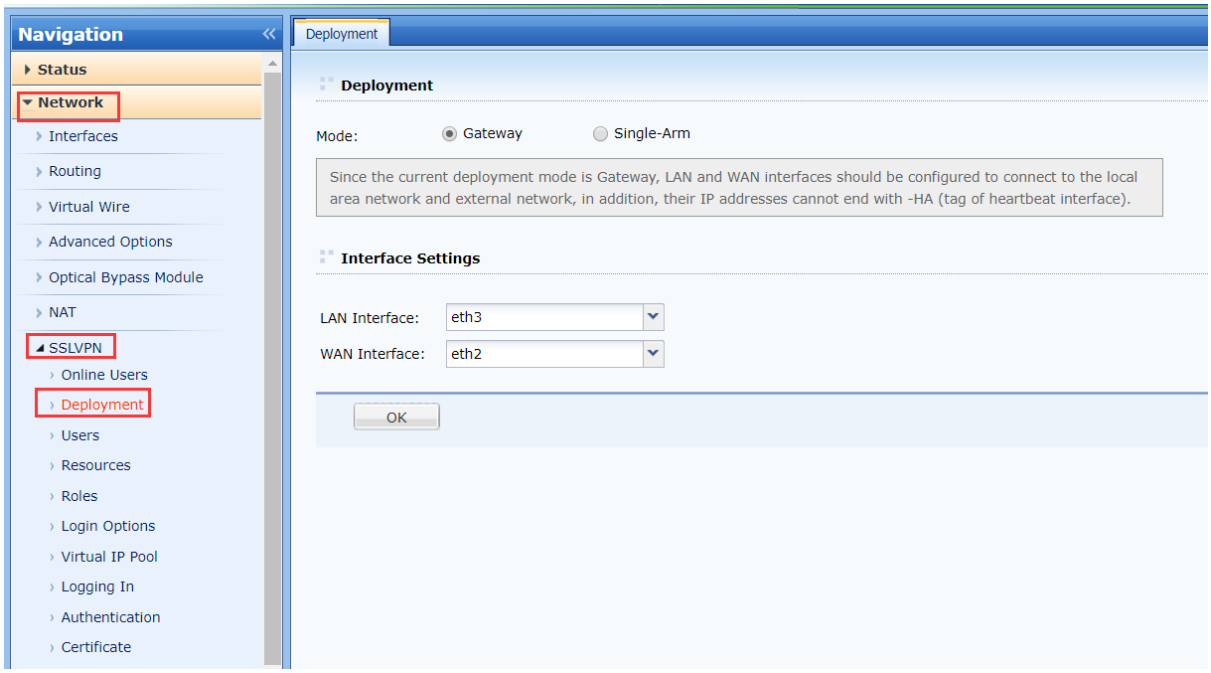
2.1 Gateway Deployment

Topology:



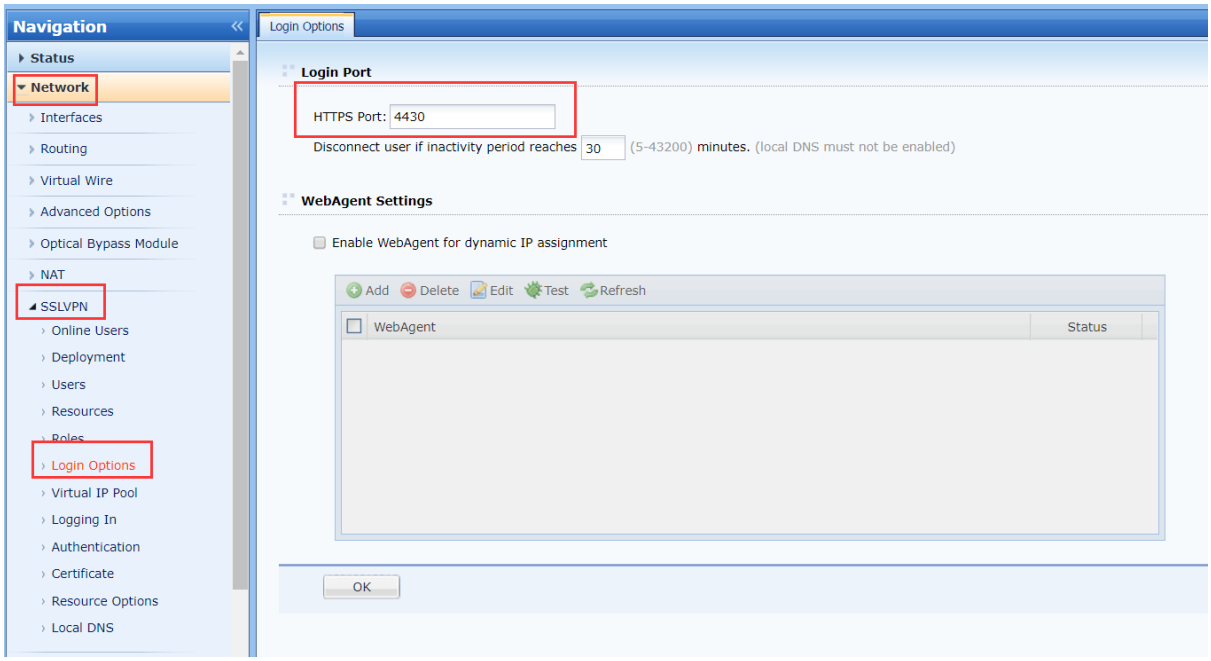
Requirement: User from public network need to use SSL VPN to access server network segment 92.168.15.0/24. Wan interface is 10.1.129.102 and Lan interface is 192.168.15.89.

2.2 Deployment mode



2.3 Login option

Default is port 4430, can modify to other port



2.4 Resouces

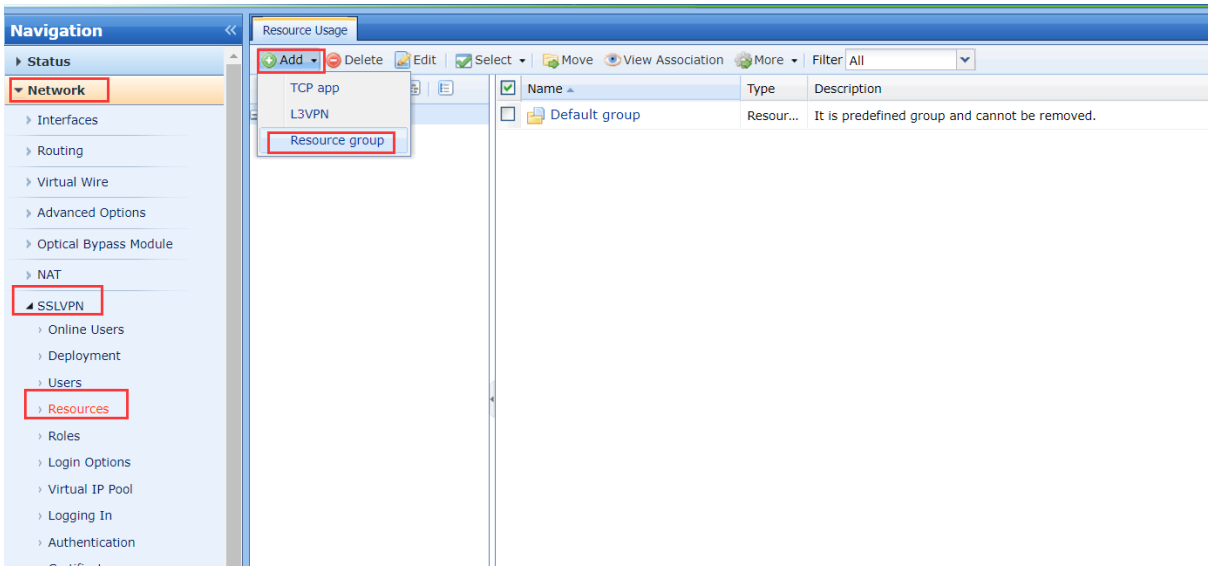
Add TCP or L3vpn resources

L3VPN resource: Client software will install virtual network card and form routing table, support all protocol.

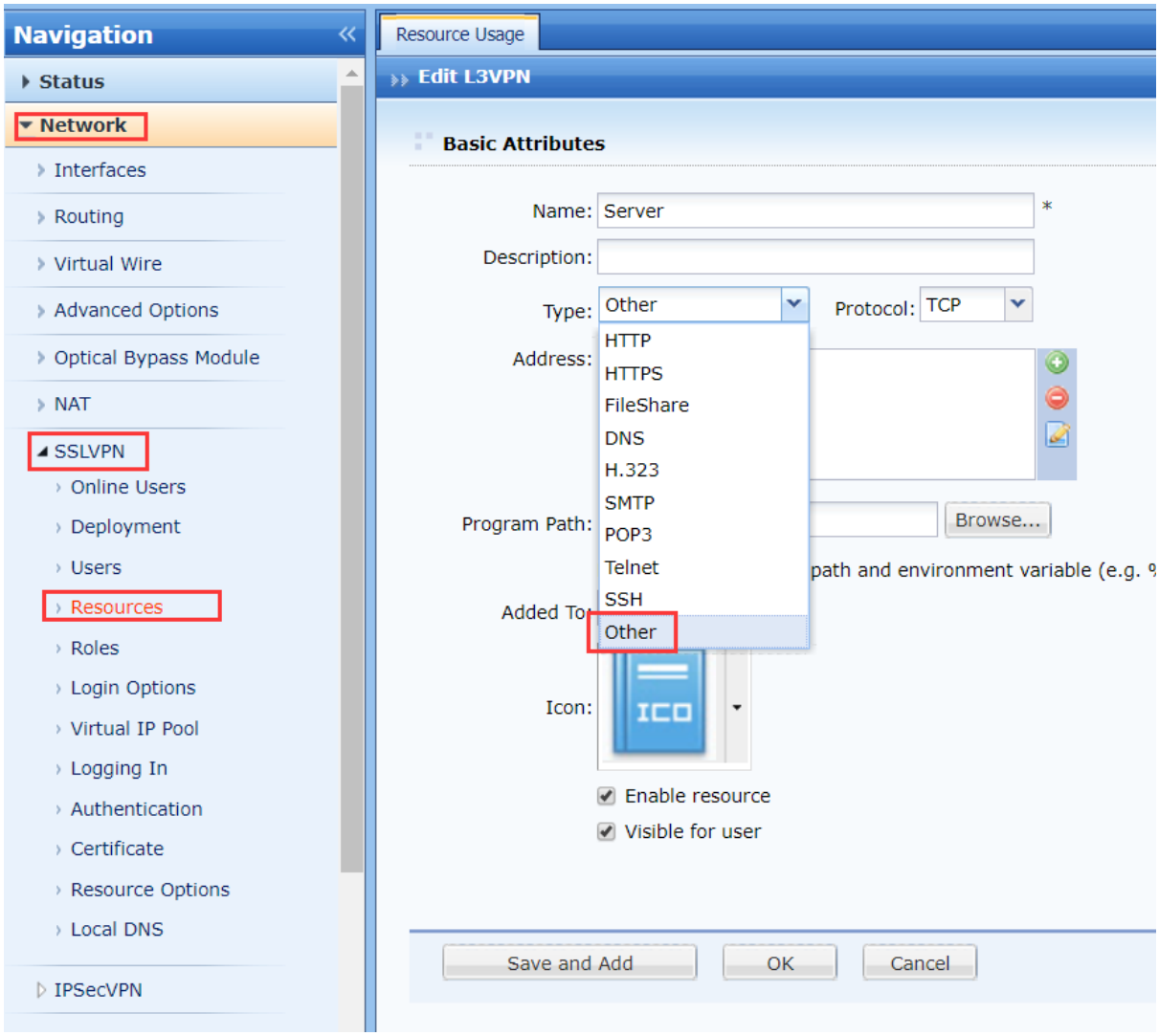
TCP resource: use proxy ie as proxy device to proxy TCP connection, only support 32 bits software, mstsc file sharing, telnet testing and etc.

Resource type:

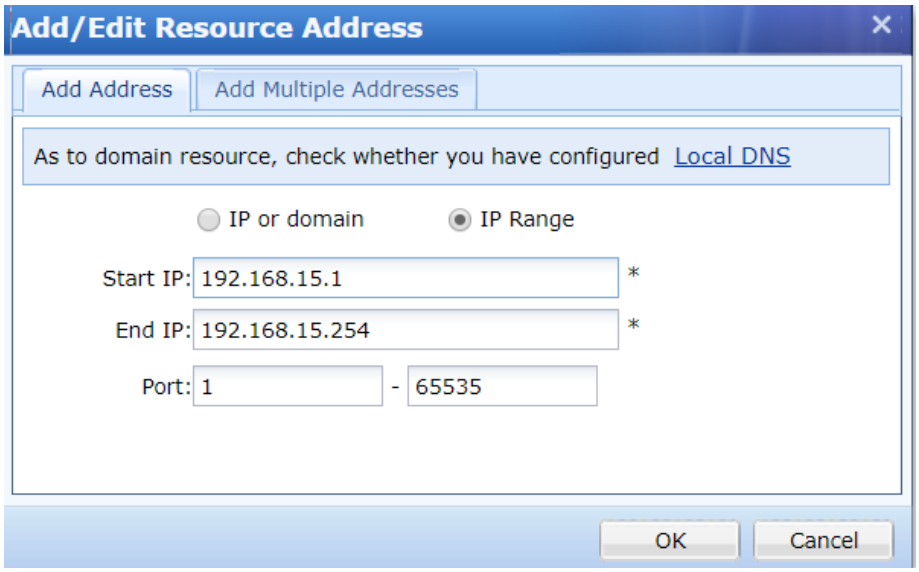
Select L3VPN first, it easy to do troubleshooting if problem occurs

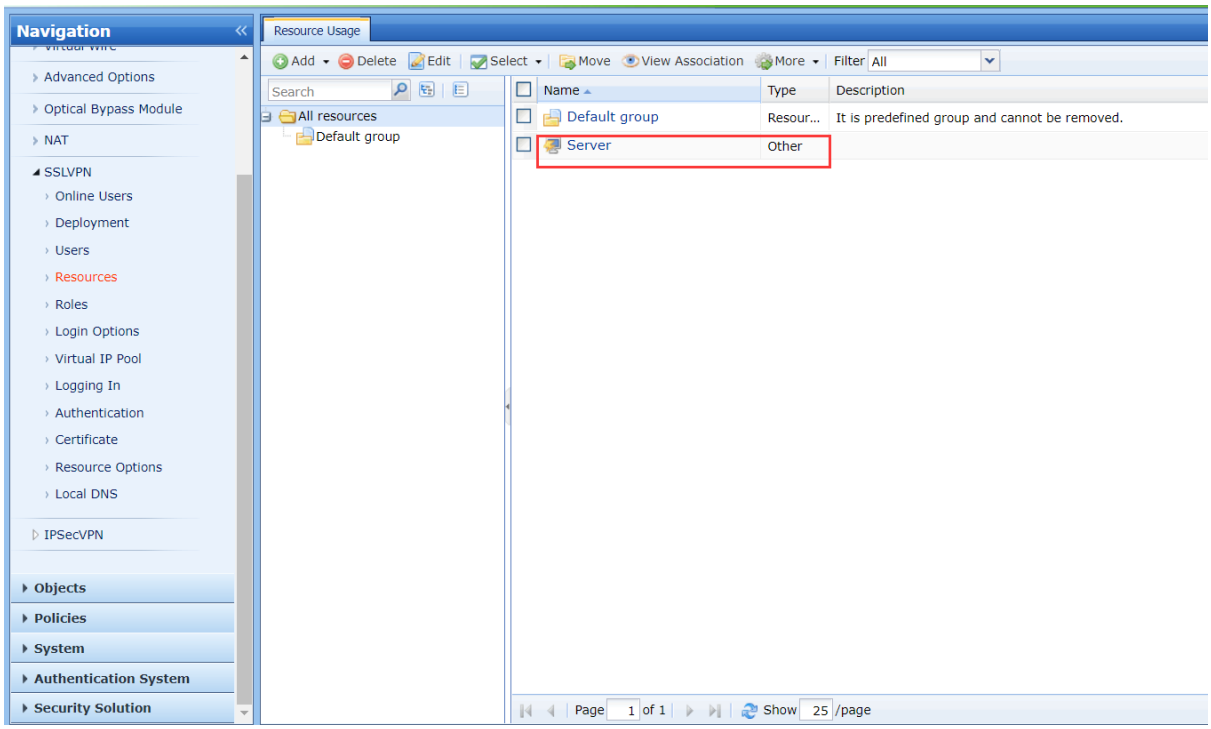


Create L3 resource, you can choose the corresponding type, other represents all types.



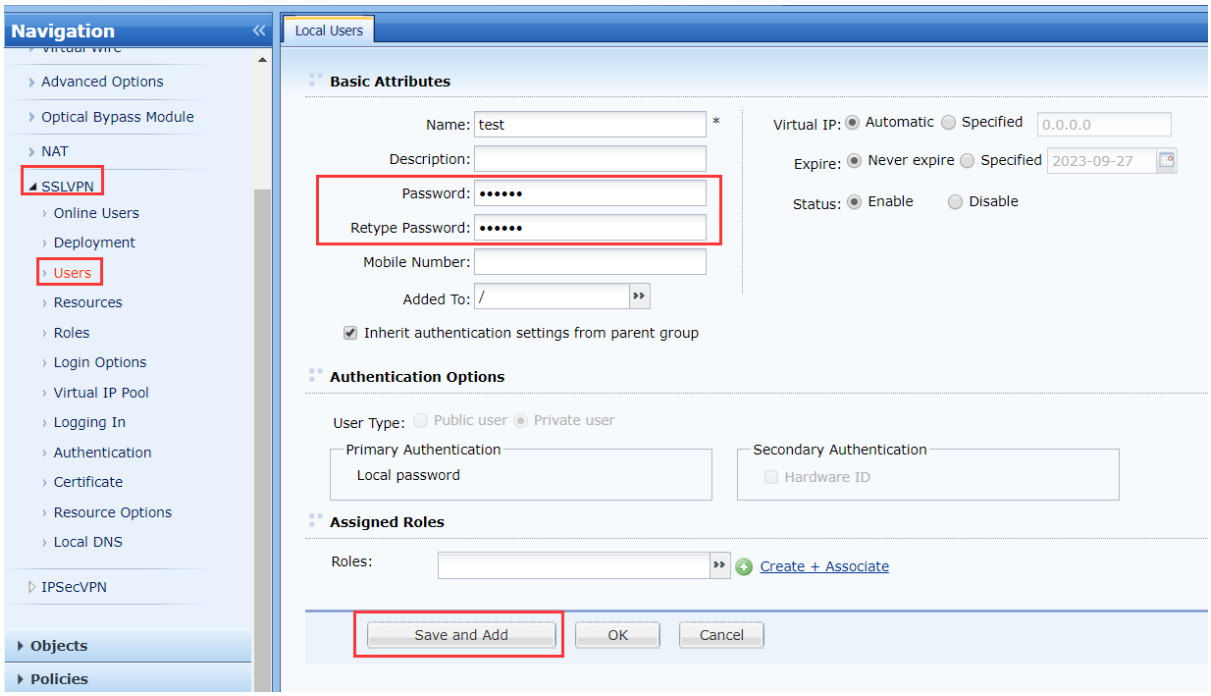
Create a name call "Server" resource, protocol can select ICMP, UDP and TCP, or all also can, address can insert the network segment, port range can from 1-6553, it shows as below.





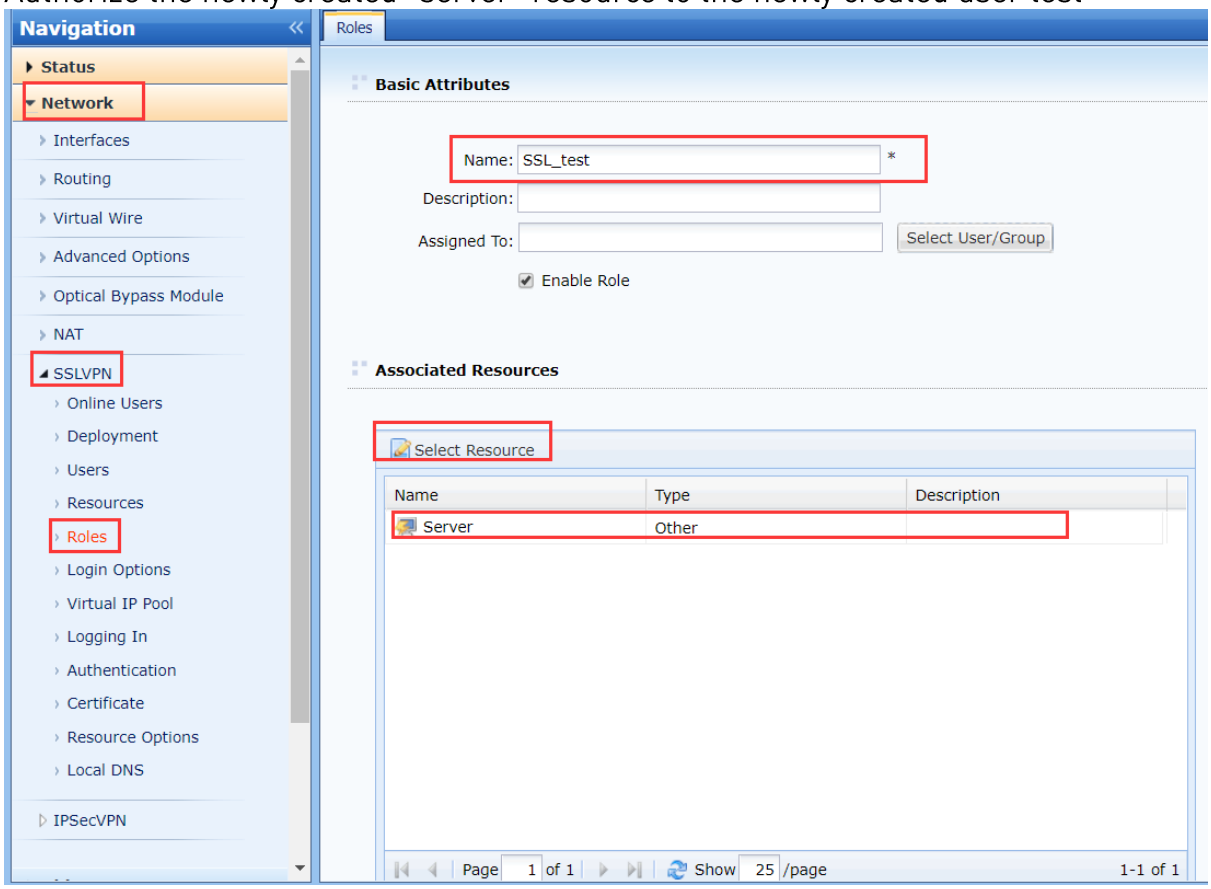
2.5 User management

Create new user account and password, other remains as default, as shown as below:



2.6 Roles

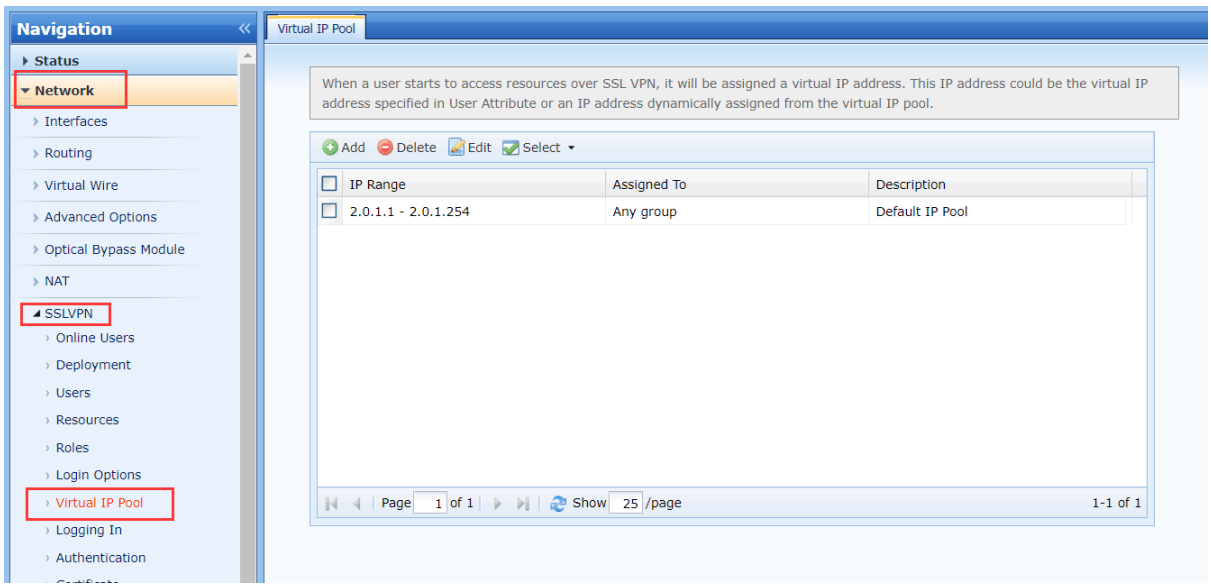
Authorize the newly created "server" resource to the newly created user test



Edit the role name, associate the newly created test user, and edit the authorized resource list (check the newly created "Server" resource), and then authorize the newly created resource to the test user.

2.7 Virtual IP pool

Randomly assign IP to the connected users.

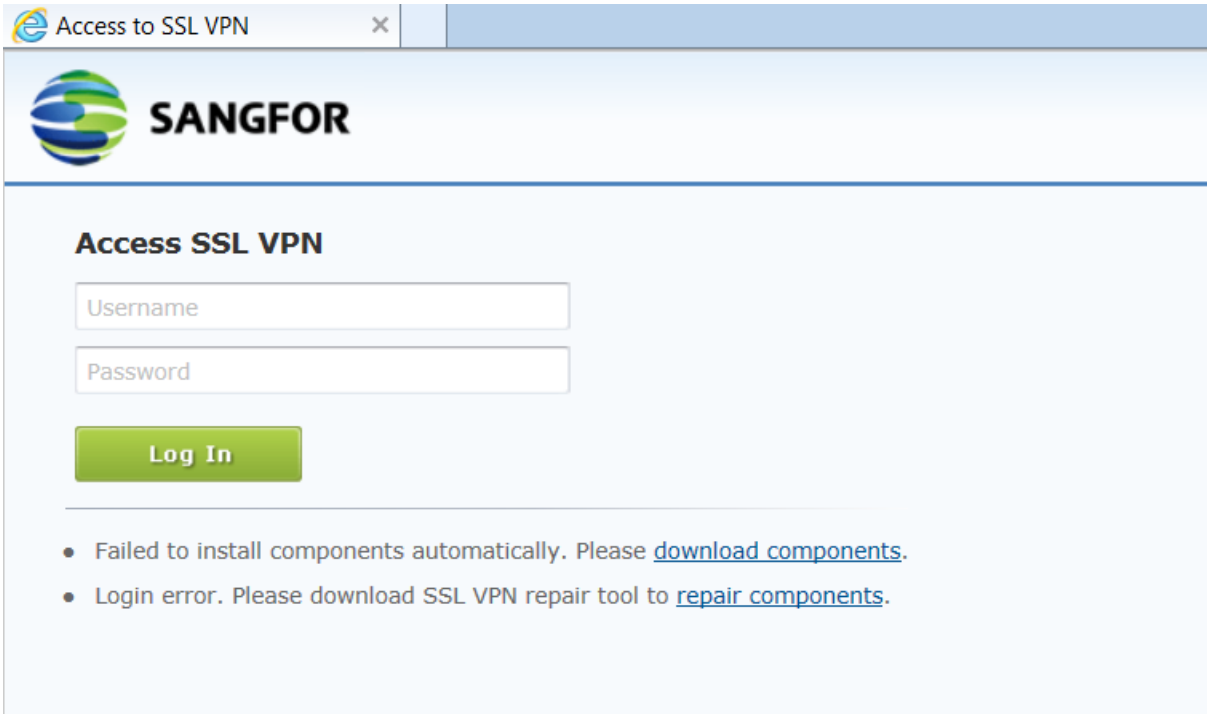


Configuration completed.

2.8 Login SSL VPN

SSLVPN login page as shown as below:

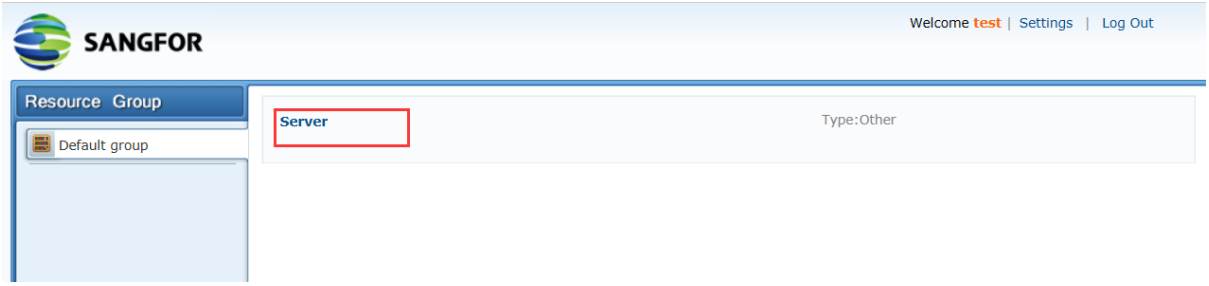
https://10.1.129.102



Insert the new added username and password then you can login.

2.9 Check the resources.

After logging in, you can see the permissions of the current user to access the resource, which is the newly created "server" resource.



Chapter 3 Precaution

3.1 If there is no resource access, first confirm whether the local computer obtains the virtual IP. The local computer can use ipconfig/all in command prompt to see

virtual NIC of the Sangfor SSLVPN is generated and whether the IP in the virtual IP pool is obtained.

3.2 The method of checking whether the virtual IP is active can also be seen in the online user in SSLVPN module, as shown in the figure: