



SANGFOR

NGAF

SSL VPN Configuration Guide

Version 8.0.5

Change Log

Date	Change Description

CONTENT

Chapter 1 SSLVPN Function Describe	4
Chapter 2 Application Scenario	4
2.1 Gateway Deployment	4
2.2 Deployment mode	5
2.3 Login option	5
2.4 Resouces	6
2.5 User management.....	8
2.6 Roles	9
2.7 Virtual IP pool	9
2.8 Login SSL VPN	10
2.9 Check the resources.	10
Chapter 3 Precaution	10

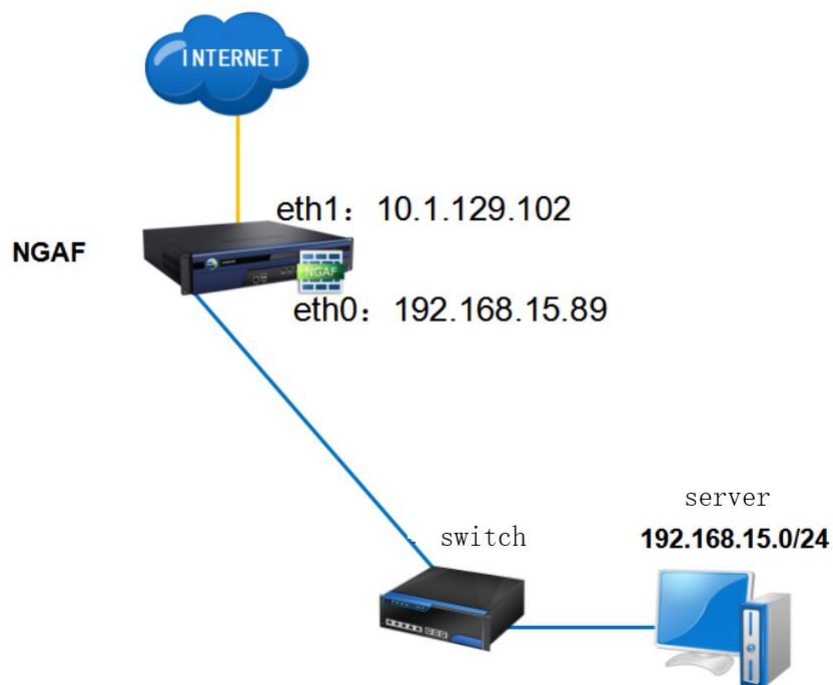
Chapter 1 SSLVPN Function Describe

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

The screenshot shows the 'Deployment' configuration page. On the left is a 'Navigation' sidebar with a tree structure. 'Network' is expanded, and 'Deployment' is selected. The main panel has a 'Deployment' section with 'Mode' set to 'Gateway' (radio button selected). A note states: 'Since the current deployment mode is Gateway, LAN and WAN interfaces should be configured to connect to the local area network and external network, in addition, their IP addresses cannot end with -HA (tag of heartbeat interface).' Below this is the 'Interface Settings' section, where 'LAN Interface' is set to 'eth3' and 'WAN Interface' is set to 'eth2'. An 'OK' button is at the bottom.

Navigation

- Status
- ▼ **Network**
 - Interfaces
 - Routing
 - Virtual Wire
 - Advanced Options
 - Optical Bypass Module
 - NAT
 - ▼ **SSLVPN**
 - Online Users
 - **Deployment**
 - Users
 - Resources
 - Roles
 - Login Options
 - Virtual IP Pool
 - Logging In
 - Authentication
 - Certificate

Deployment

Mode: ☒ Gateway ☐ Single-Arm

Since the current deployment mode is Gateway, LAN and WAN interfaces should be configured to connect to the local area network and external network, in addition, their IP addresses cannot end with -HA (tag of heartbeat interface).

Interface Settings

LAN Interface:

WAN Interface:

2.3 Login option

Default is port 4430, can modify to other port

The screenshot shows the 'Login Options' configuration page. On the left is a 'Navigation' sidebar. 'Network' is expanded, 'SSLVPN' is selected, and 'Login Options' is selected. The main panel has a 'Login Port' section with 'HTTPS Port' set to '4430'. Below it, a text field shows 'Disconnect user if inactivity period reaches 30 (5-43200) minutes. (local DNS must not be enabled)'. The 'WebAgent Settings' section has a checkbox 'Enable WebAgent for dynamic IP assignment' which is unchecked. Below this is a table with columns 'WebAgent' and 'Status'. The table is empty. An 'OK' button is at the bottom.

Navigation

- Status
- ▼ **Network**
 - Interfaces
 - Routing
 - Virtual Wire
 - Advanced Options
 - Optical Bypass Module
 - NAT
 - ▼ **SSLVPN**
 - Online Users
 - Deployment
 - Users
 - Resources
 - Roles
 - **Login Options**
 - Virtual IP Pool
 - Logging In
 - Authentication
 - Certificate
 - Resource Options
 - Local DNS

Login Options

Login Port

HTTPS Port:

Disconnect user if inactivity period reaches (5-43200) minutes. (local DNS must not be enabled)

WebAgent Settings

☐ Enable WebAgent for dynamic IP assignment

WebAgent	Status
----------	--------

2.4 Resources

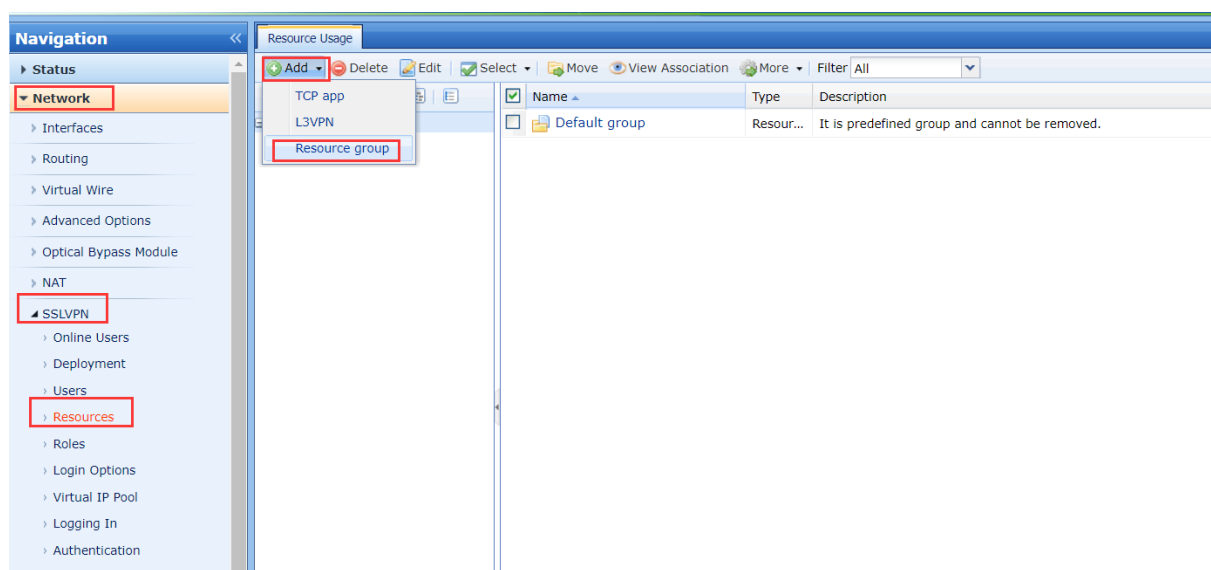
Add TCP or L3vpn resources

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.

Navigation

- Status
- ▼ **Network**
 - Interfaces
 - Routing
 - Virtual Wire
 - Advanced Options
 - Optical Bypass Module
 - NAT
 - ▼ **SSLVPN**
 - Online Users
 - Deployment
 - Users
 - **Resources**
 - Roles
 - Login Options
 - Virtual IP Pool
 - Logging In
 - Authentication
 - Certificate
 - Resource Options
 - Local DNS
 - IPSecVPN

Resource Usage

Edit L3VPN

Basic Attributes

Name: Server *

Description:

Type: Other ▼ Protocol: TCP ▼

Address:

Program Path: Browse...

Added To:

Icon: ICO

☒ Enable resource

☒ Visible for user

Save and Add OK Cancel

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.

Add/Edit Resource Address

Add Address Add Multiple Addresses

As to domain resource, check whether you have configured [Local DNS](#)

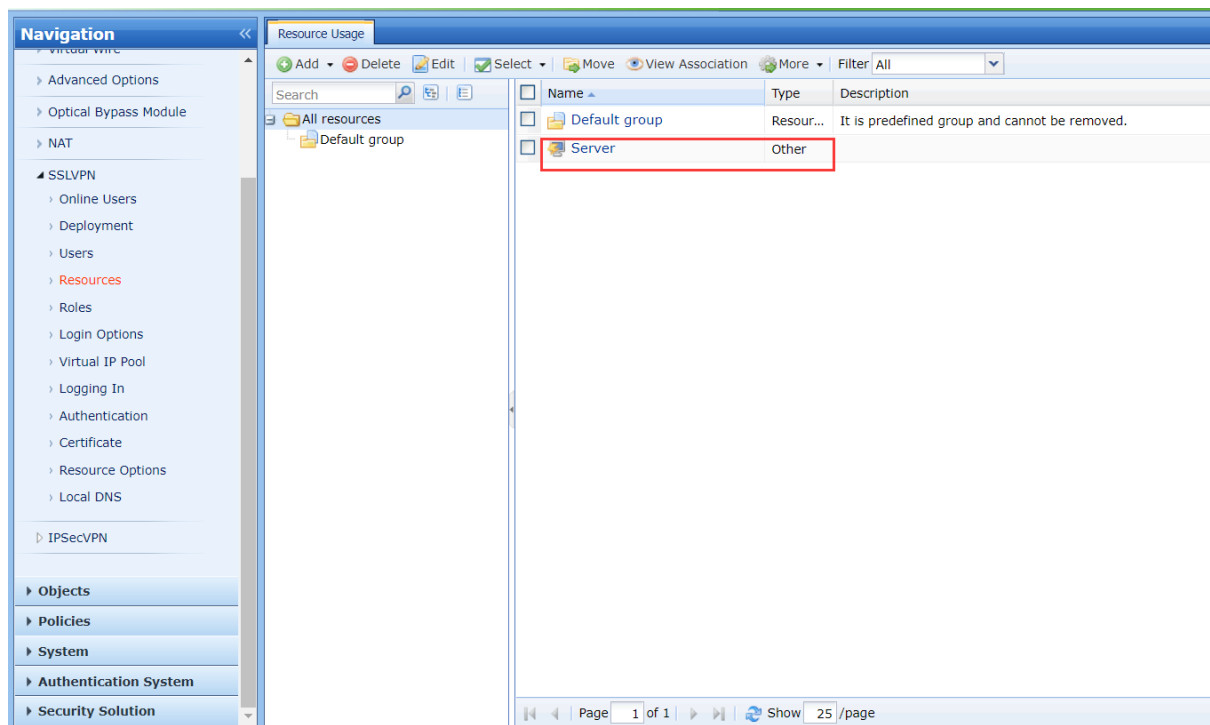
☐ IP or domain ☒ IP Range

Start IP: 192.168.15.1 *

End IP: 192.168.15.254 *

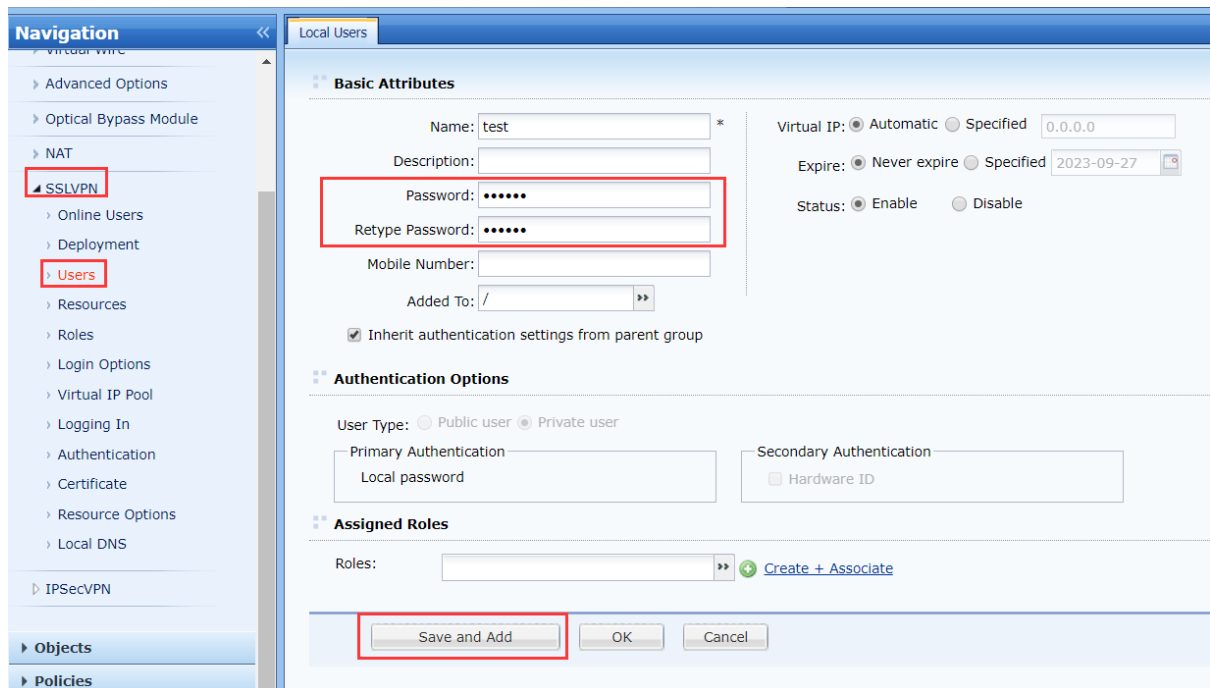
Port: 1 - 65535

OK Cancel



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

The screenshot shows the 'Roles' configuration page. On the left is a 'Navigation' pane with a tree structure. The 'Roles' item is highlighted. The main area is titled 'Roles' and contains two sections: 'Basic Attributes' and 'Associated Resources'.

Basic Attributes:

- Name:** SSL_test *
- Description:** (empty field)
- Assigned To:** (empty field) with a 'Select User/Group' button
- ☒ Enable Role

Associated Resources:

A 'Select Resource' button is at the top. Below it is a table with the following data:

Name	Type	Description
Server	Other	

At the bottom of the page, there is a pagination bar showing 'Page 1 of 1', 'Show 25 /page', and '1-1 of 1'.

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.

The screenshot shows the 'Virtual IP Pool' configuration page. On the left is a 'Navigation' pane with a tree structure. The 'Virtual IP Pool' item is highlighted. The main area is titled 'Virtual IP Pool' and contains a text box at the top and a table below.

Text Box:

When a user starts to access resources over SSL VPN, it will be assigned a virtual IP address. This IP address could be the virtual IP address specified in User Attribute or an IP address dynamically assigned from the virtual IP pool.

Table:

At the top of the table are buttons: Add, Delete, Edit, and Select. The table has the following data:

IP Range	Assigned To	Description
<input type="checkbox"/> 2.0.1.1 - 2.0.1.254	Any group	Default IP Pool

At the bottom of the page, there is a pagination bar showing 'Page 1 of 1', 'Show 25 /page', and '1-1 of 1'.

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.

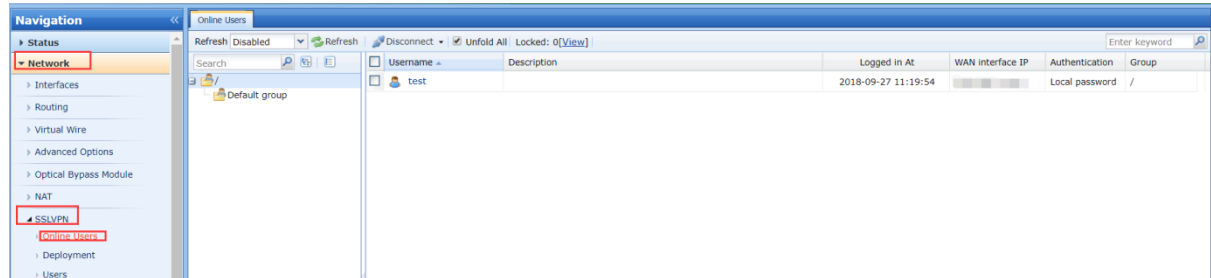
After logging in, you can see the permissions of the current user to access the resource, which is the newly created "server" resource.

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:





Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

The information in this document is subject to change without notice.

To obtain the latest version, contact the international service center of SANGFOR Technologies Inc