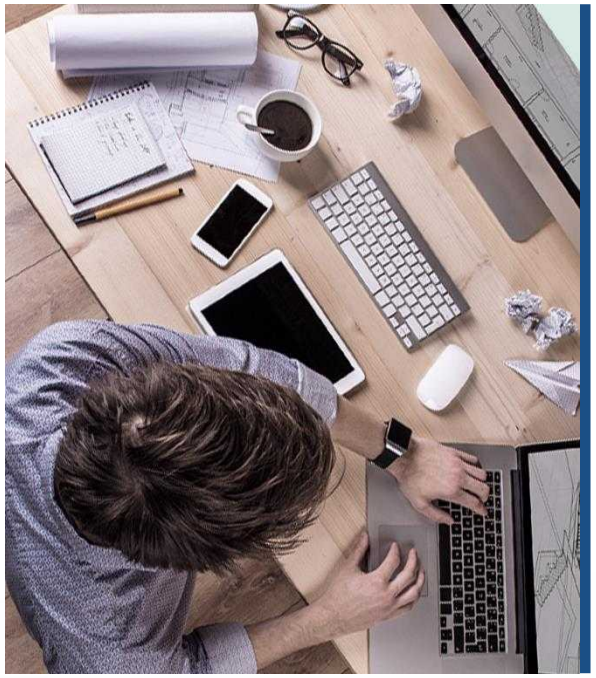
SANGFOR

Sangfor NSF V8.0.85 Associate

VPN



1. IPSec VPN
2. Sangfor VPN
3. SSL VPN

PART 1 IPSec VPN

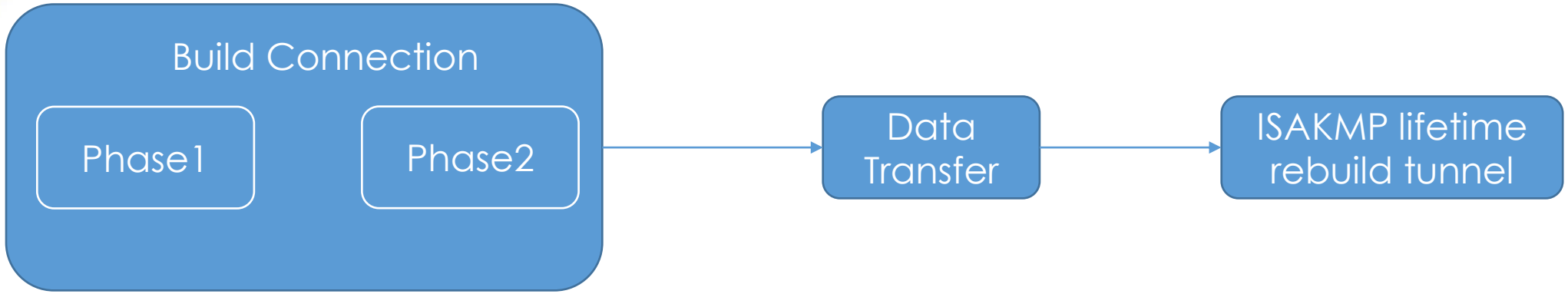
IPSEC VPN

A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

Internet Protocol Security (IPsec) is a network protocol suite that authenticates and encrypts the packets of data sent over a network. IPsec supports network-level peer authentication, **data-origin authentication**, **data integrity**, **data confidentiality (encryption)**, and replay protection.

All Sangfor security products support the IPsec VPN.

IPSEC VPN

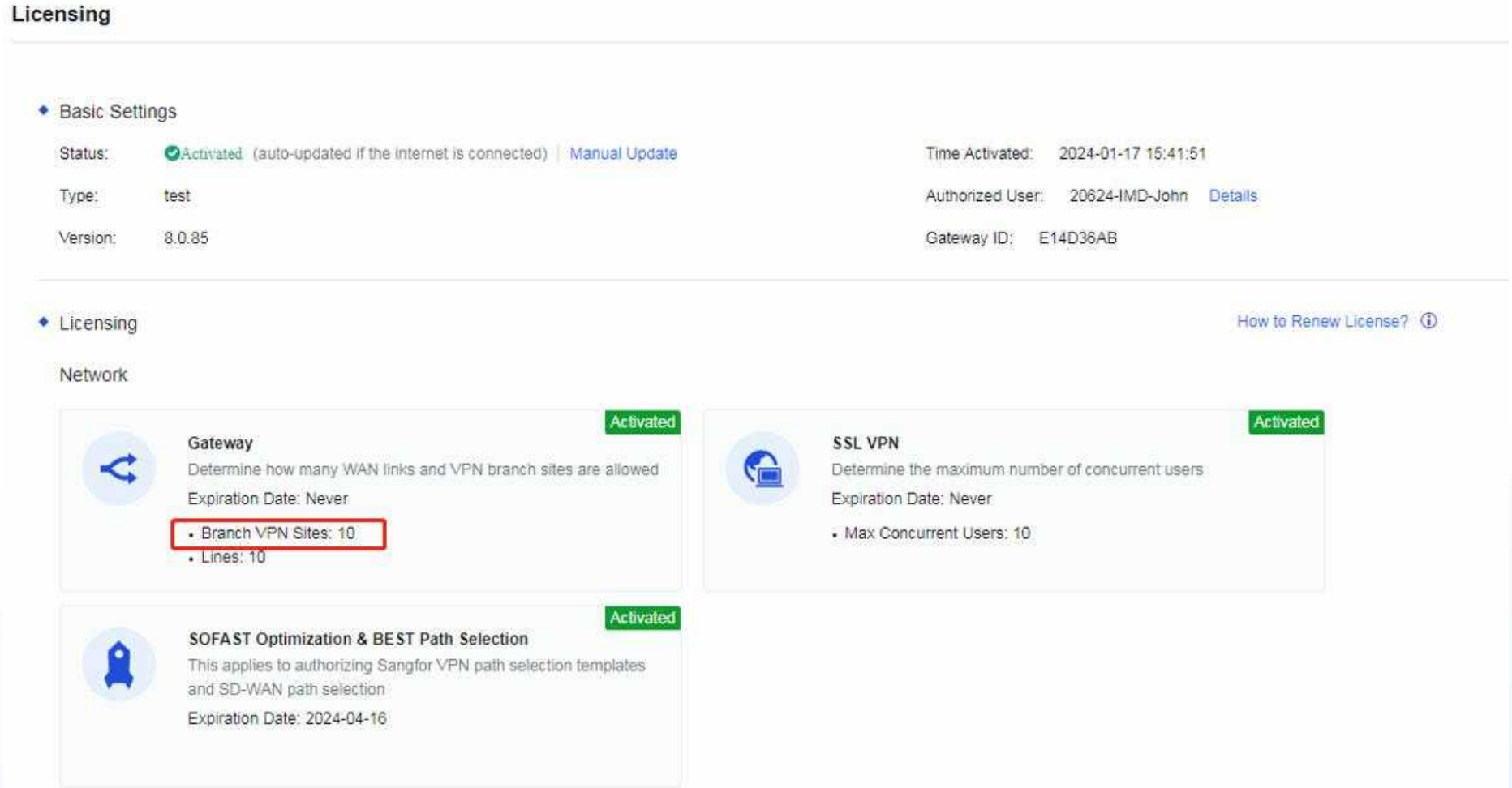


Phase1:
1. IKE version: 1/2
2. Mode: Main/Aggressive
3. SA exchange: Authentication algorithm/Encryption algorithm/DH Group/ISAKMP life time
4. Exchange Pre-shared key
5. Exchange and Verify ID
6. Other: NAT/DPD

Phase2:
1. Protocol :AH/ESP
2. PFS
3. Encryption : DES/3DES/AES128 Hash:MD5/SHA
4. SA lifetime
5. Local IP address and Peer IP address

IPSEC VPN

1. NSF must have Branch VPN Sites license to establish a IPsec VPN. Another requirement, the encrypted network segments in both sides of IPSec VPN shouldn't conflict.

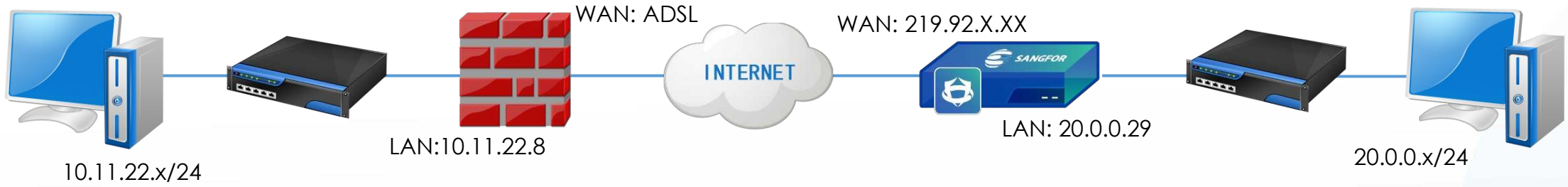


IPSEC VPN Case Study

Customer wants to communicate in two sites by using internal IP address.

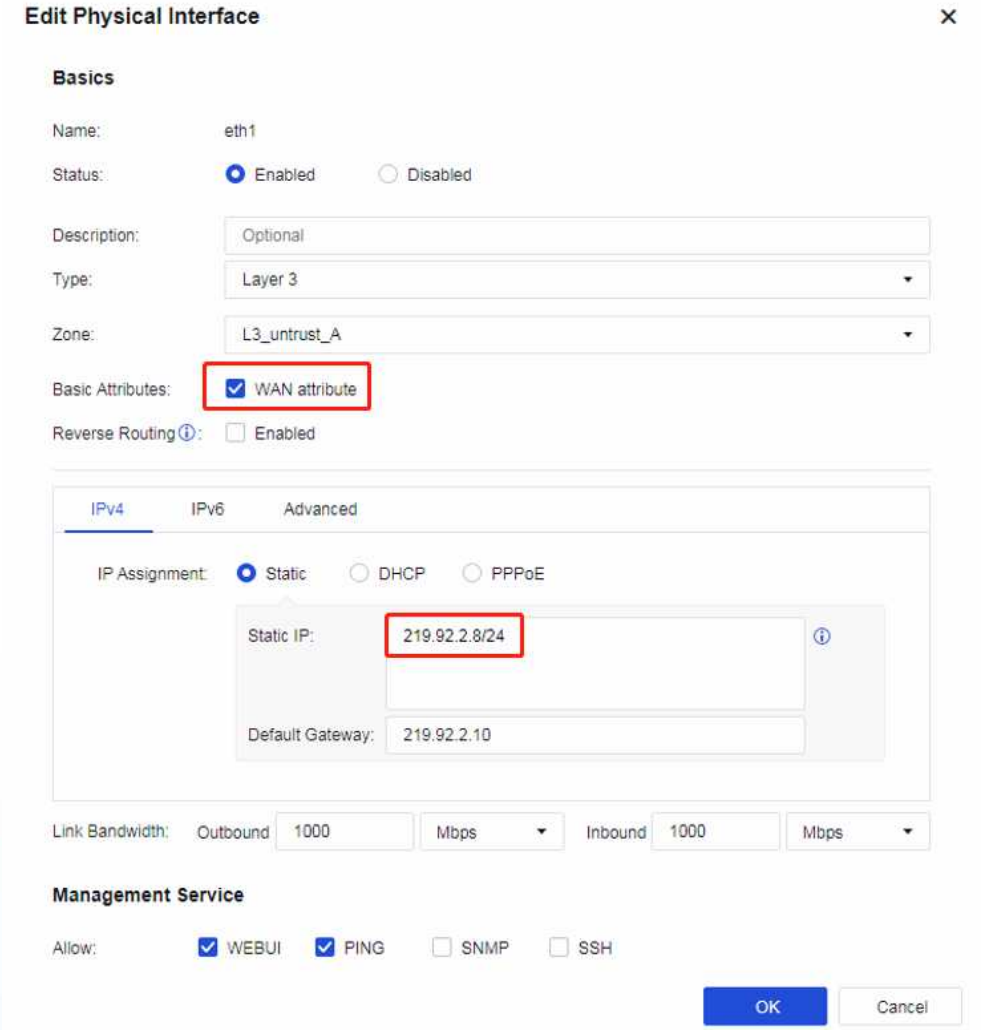
Sangfor:
Static public IP, directly connect to internet.

Fortinet/FortiGate:
ADSL, directly connect to internet.
Customer want to side intranet visit each other
via IPSec VPN

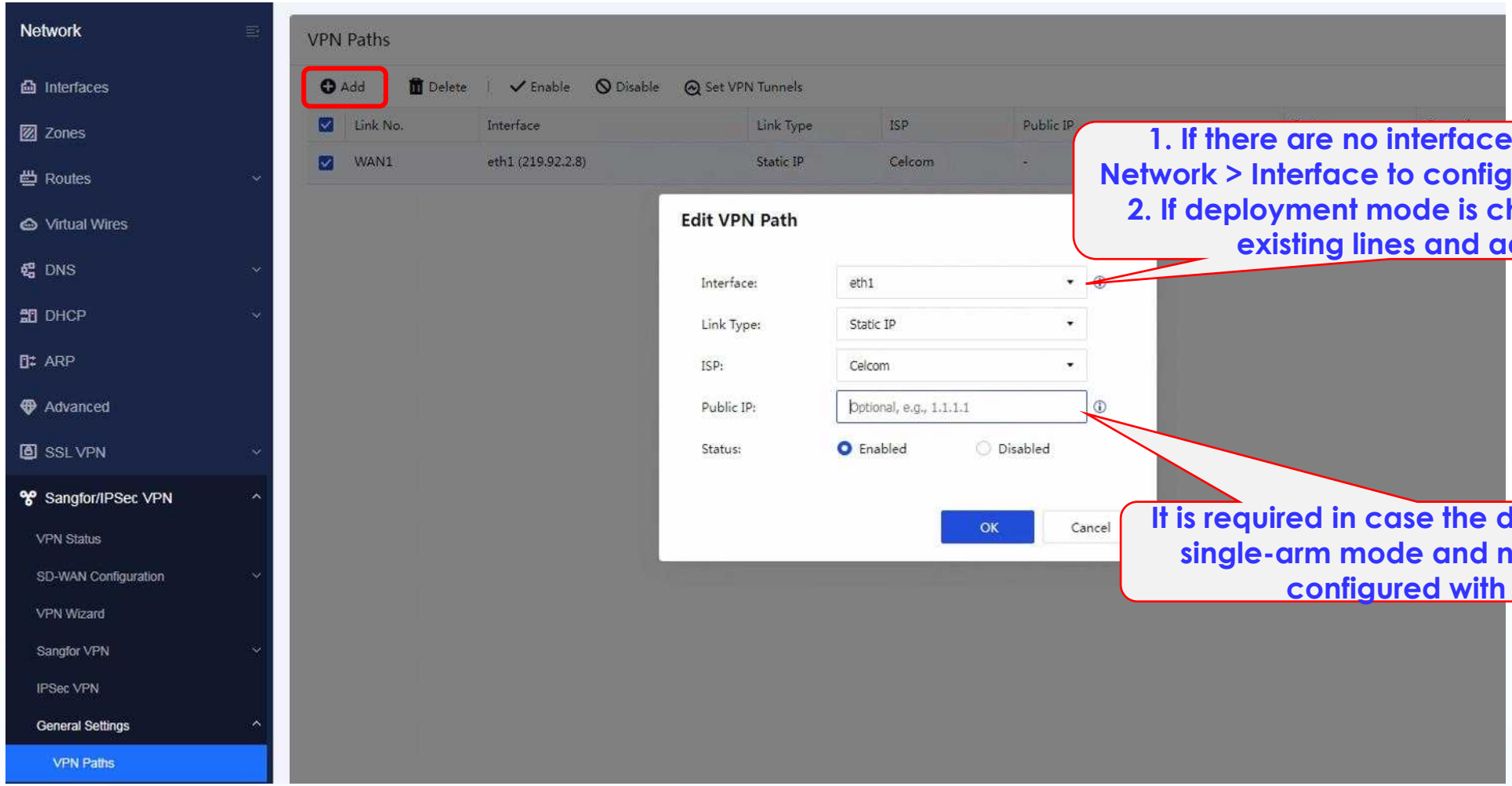


Precautions: Dynamic IP needs to apply for a domain name and use Aggressive mode.

1. Configure the interface and the zone, Configuration path: **Network > Interfaces**.



2. Configure the VPN Path, go to **Network > Sangfor/IPSec VPN > General Settings > VPN Pat**

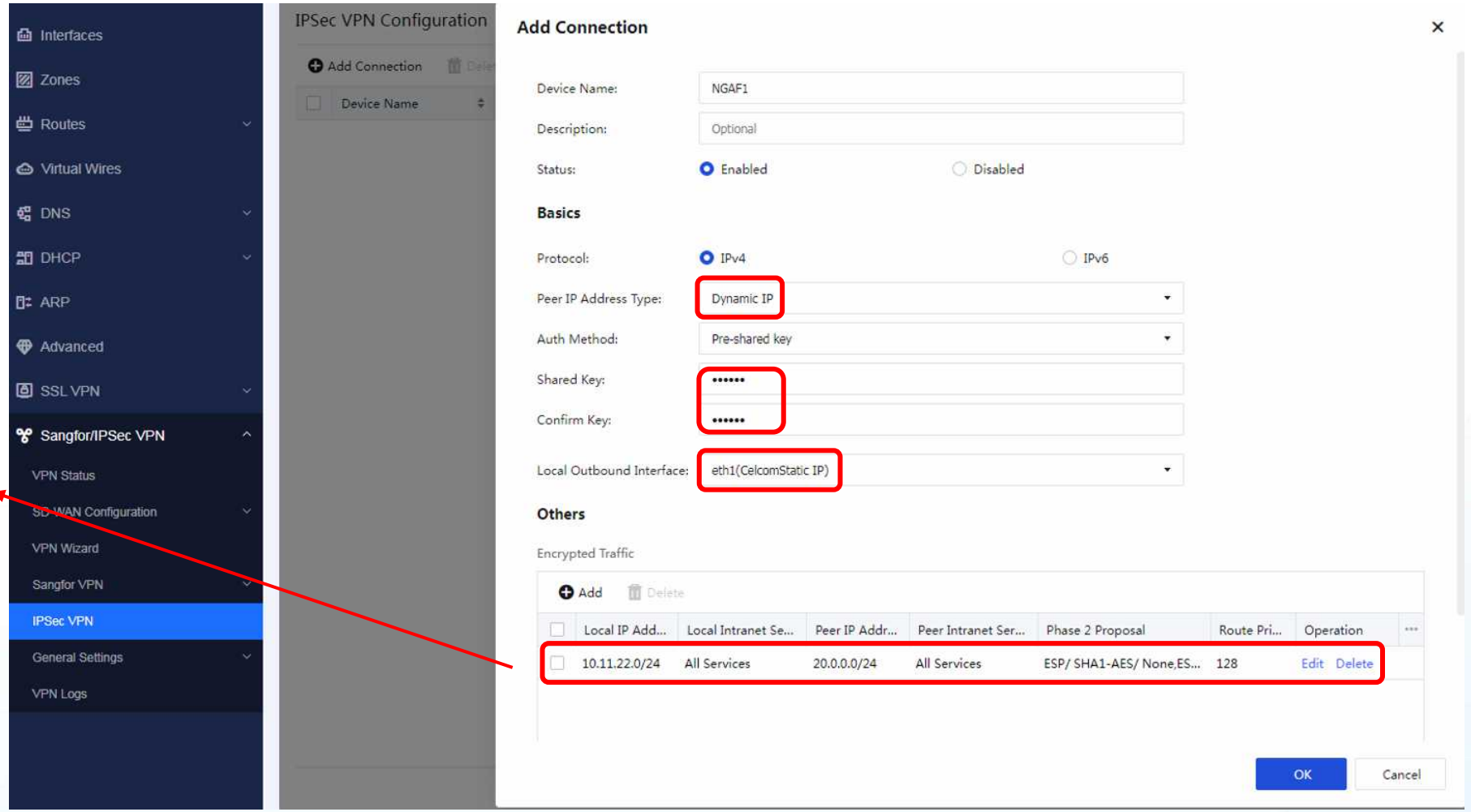


3. Basics

Configuration Path: **Network > Sangfor/IPSec VPN > IPSec VPN**

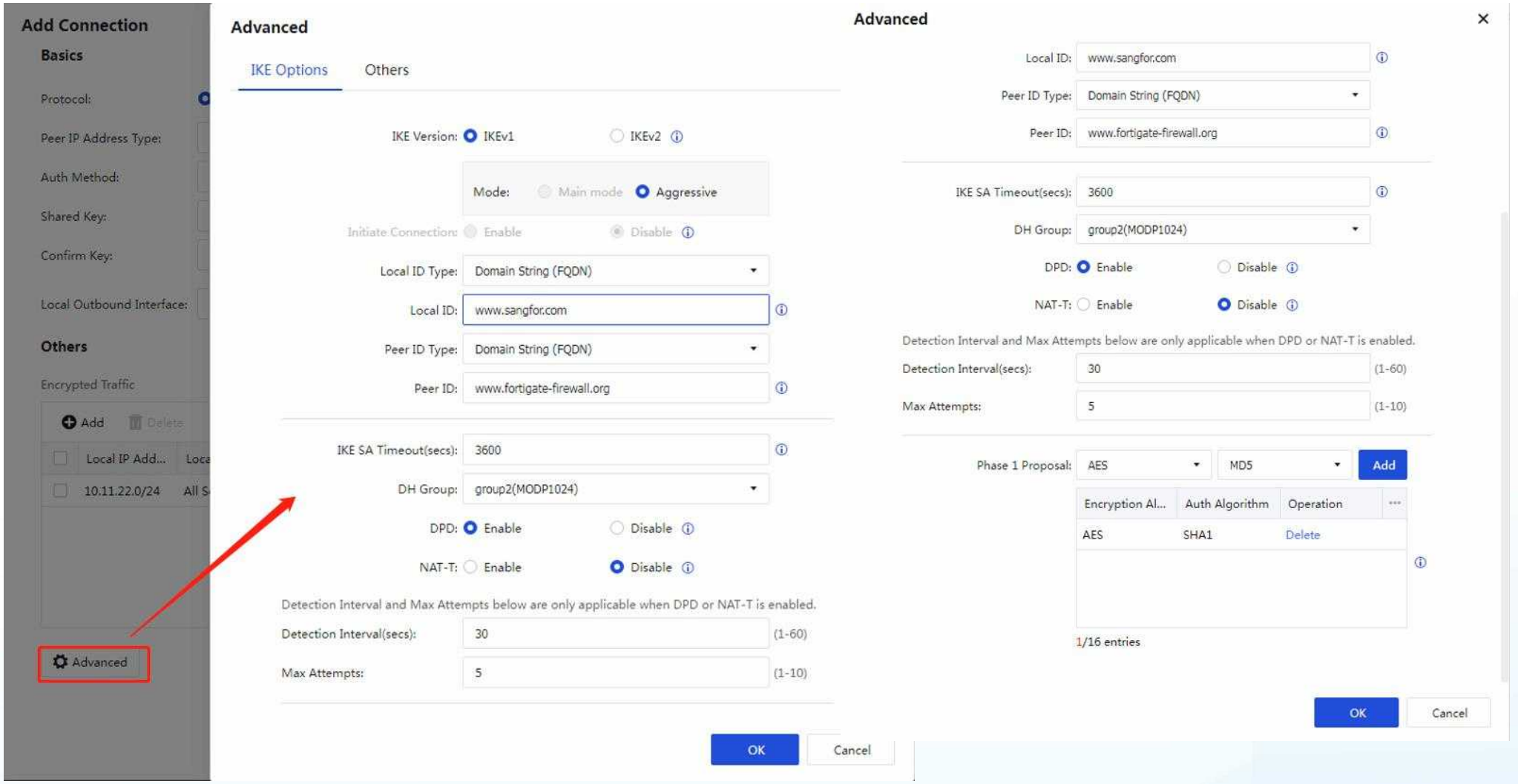
Local IP Address: Input the intranet network segment of the local device.

Peer IP Address: Input the intranet network segment of the peer device.

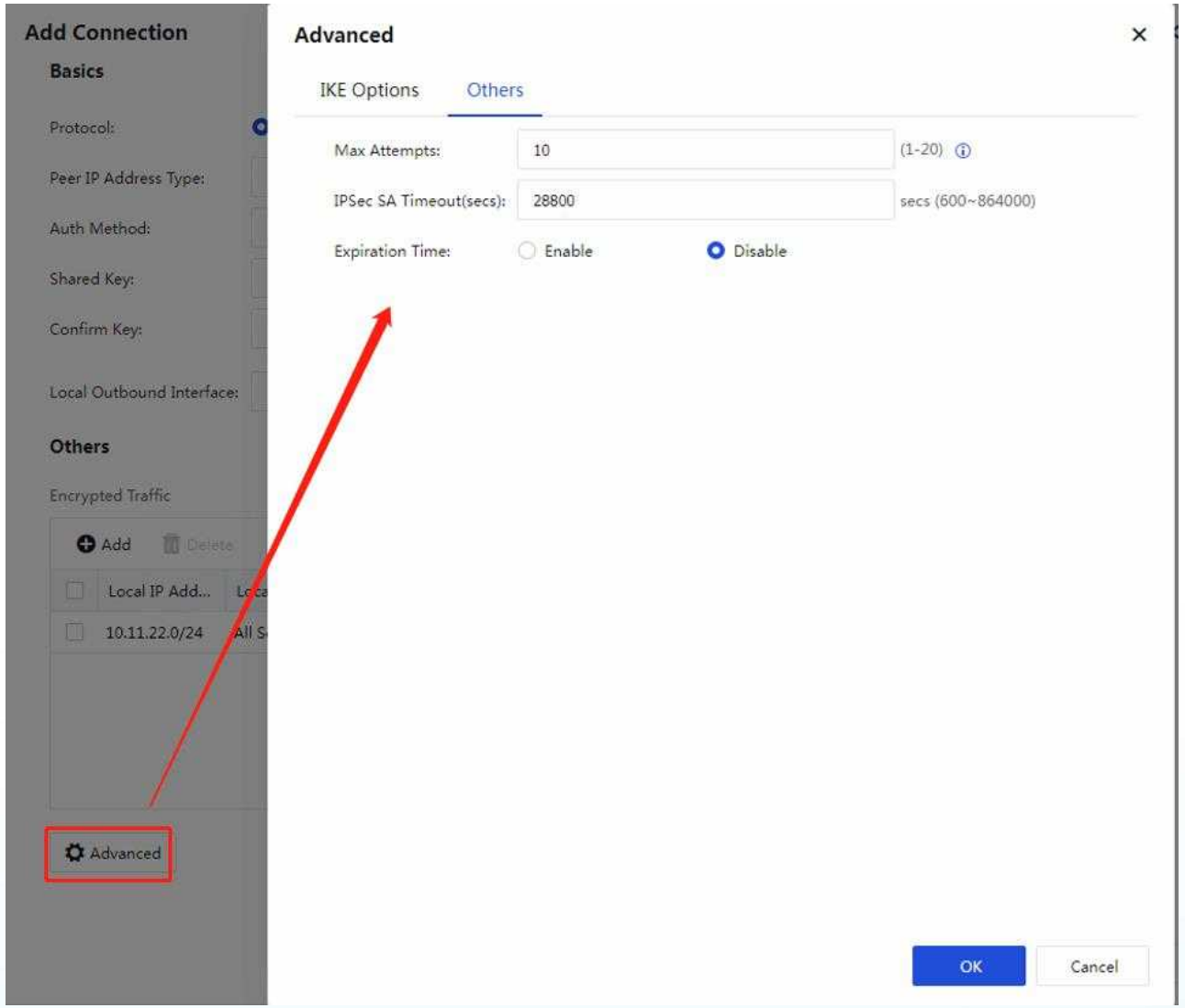


SANGFOR

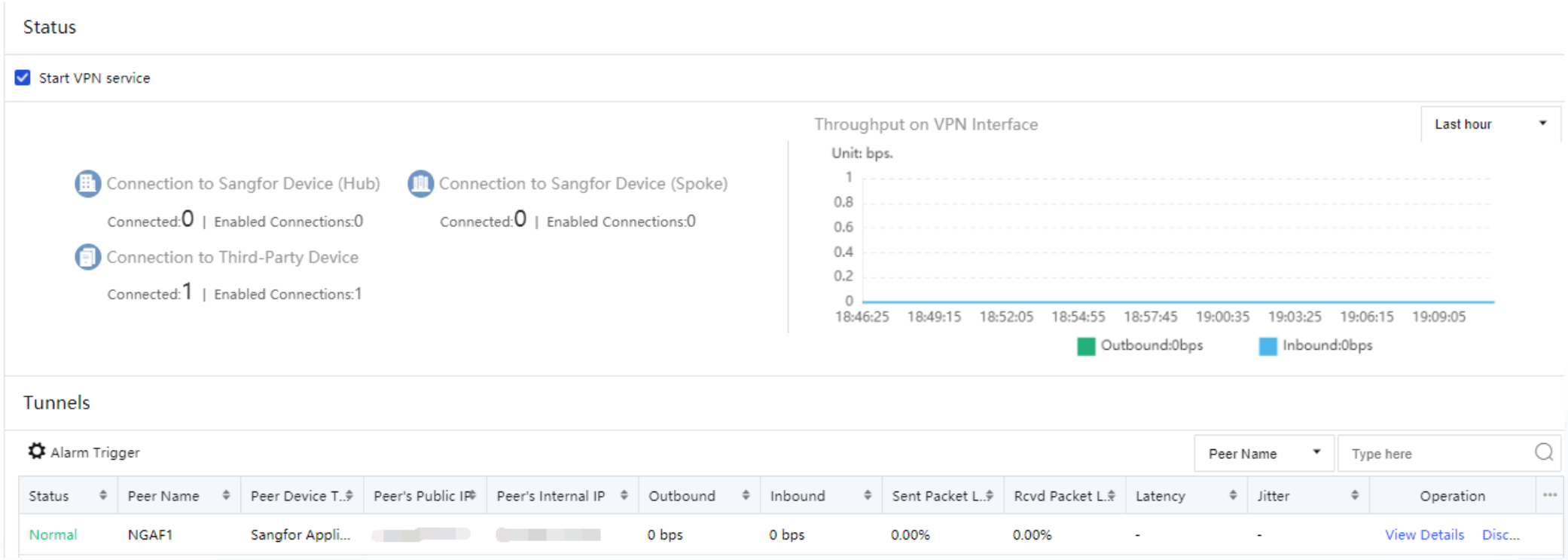
4. IKE Options



5. Other Options



6. After successfully configuration, we can see the tunnel in the **IPSec VPN > Status**.



PART 2 Sangfor VPN

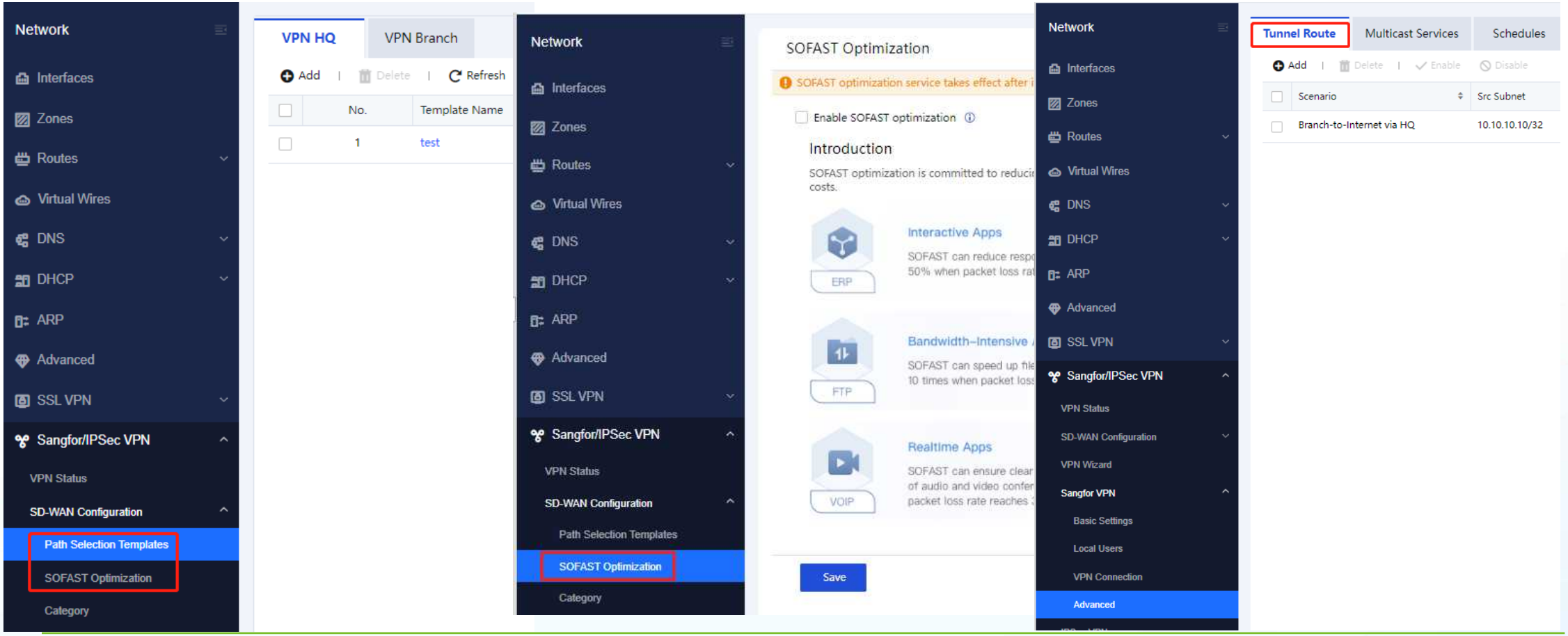
Sangfor VPN

Sangfor NSF provides two types of VPN connections namely, standard IPSEC VPN, and a self-developed SANGFOR VPN, providing the device-to-device connection. SANGFOR VPN has the following advantages in comparison to standard IPSEC VPN:

1. Support both ends that are non-fixed IP public network environment.
2. Existence of VPN multi-line technology to achieve VPN link load balancing.
3. Branch users are connected through the HQ Internet to achieve unified control of the HQ via the tunnel route.
4. The tunnel NAT technology are used to solve problems of multiple branch network which IP segments conflict.

Sangfor VPN

Sangfor VPN is a core component for SD-WAN scenario in NSF, and many features shown as below, are based on Sangfor VPN.



Sangfor VPN

Usages of Sangfor VPN:

HQ:
Provides VPN access services, and provides access to account verification of other VPN users. Sangfor VPN in HQ side requires WEBAGENT configuration and VPN account for access. Generally, server side of the network is HQ.

Branch:
Access to HQ side. Generally, branch as client network.

A VPN device can act as a HQ or branch.

Sangfor VPN

The term of Sangfor VPN:

Webagent:
For SANGFOR VPN interconnection, branch and mobile users look for HQ address to establish a VPN connection.

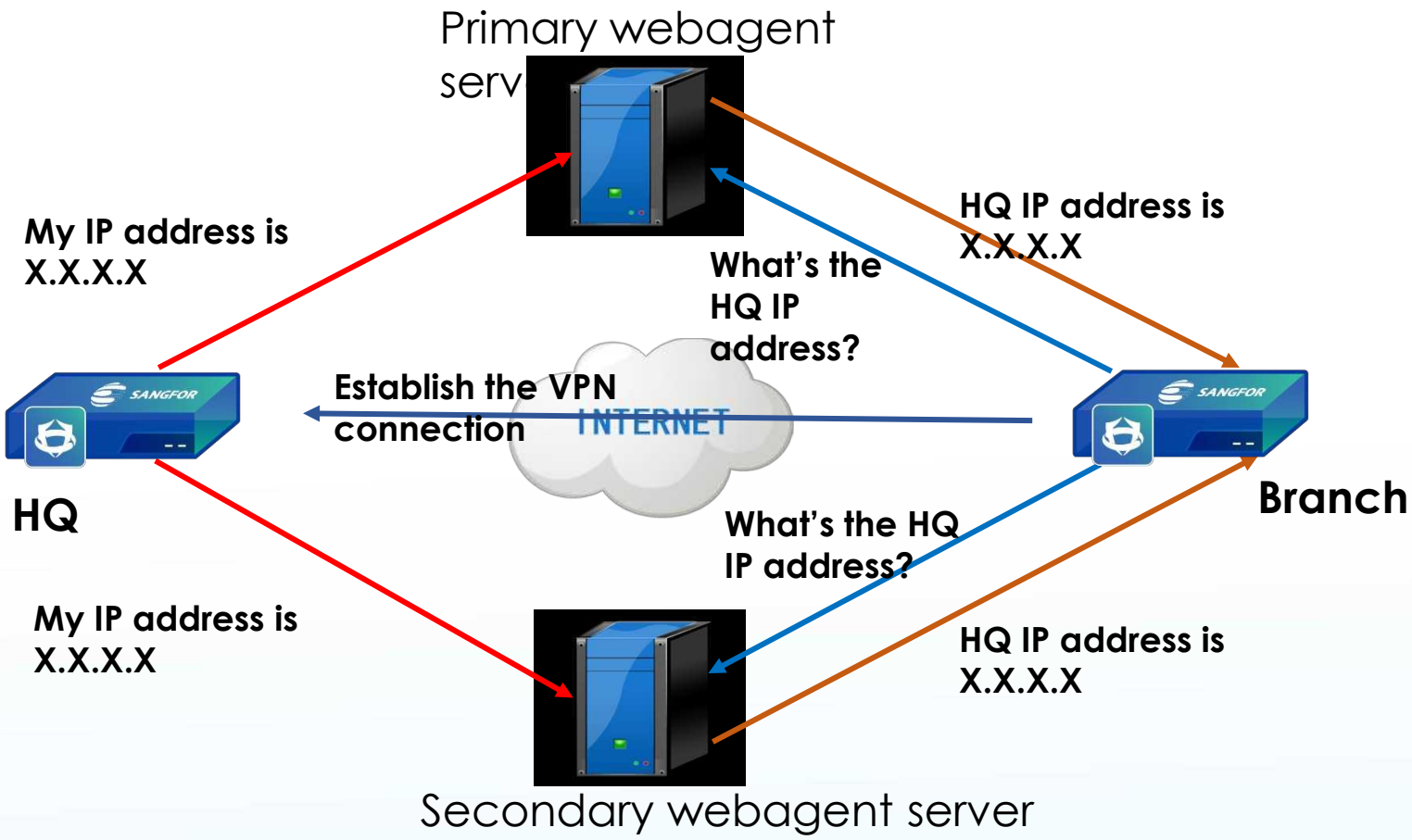
You can configure webagent in several ways:
1. IP: Port, eg.123.123.123.123:4009
Applicable to HQ VPN device that has a fixed public IP address of the environment.

2. IP1 # IP2: Port, such as 123.123.123.123 # 221.221.221.221: 4009
HQ VPN device that has multiple lines with fixed IP, and require VPN backups or for load balance.

3. Web URL format, such as: webagent.sangfor.com.cn/webagent/123.php
HQ VPN device that has no fixed IP environment, such as ADSL lines.

WEBAGENT addressing process:

(During the addressing process, information is encrypted with DES.)



Sangfor VPN

The basic configurations for establishing a VPN connection between HQ and branch or mobile are as follow:

(1) HQ: Need to configure VPN path, webagent, and local users.

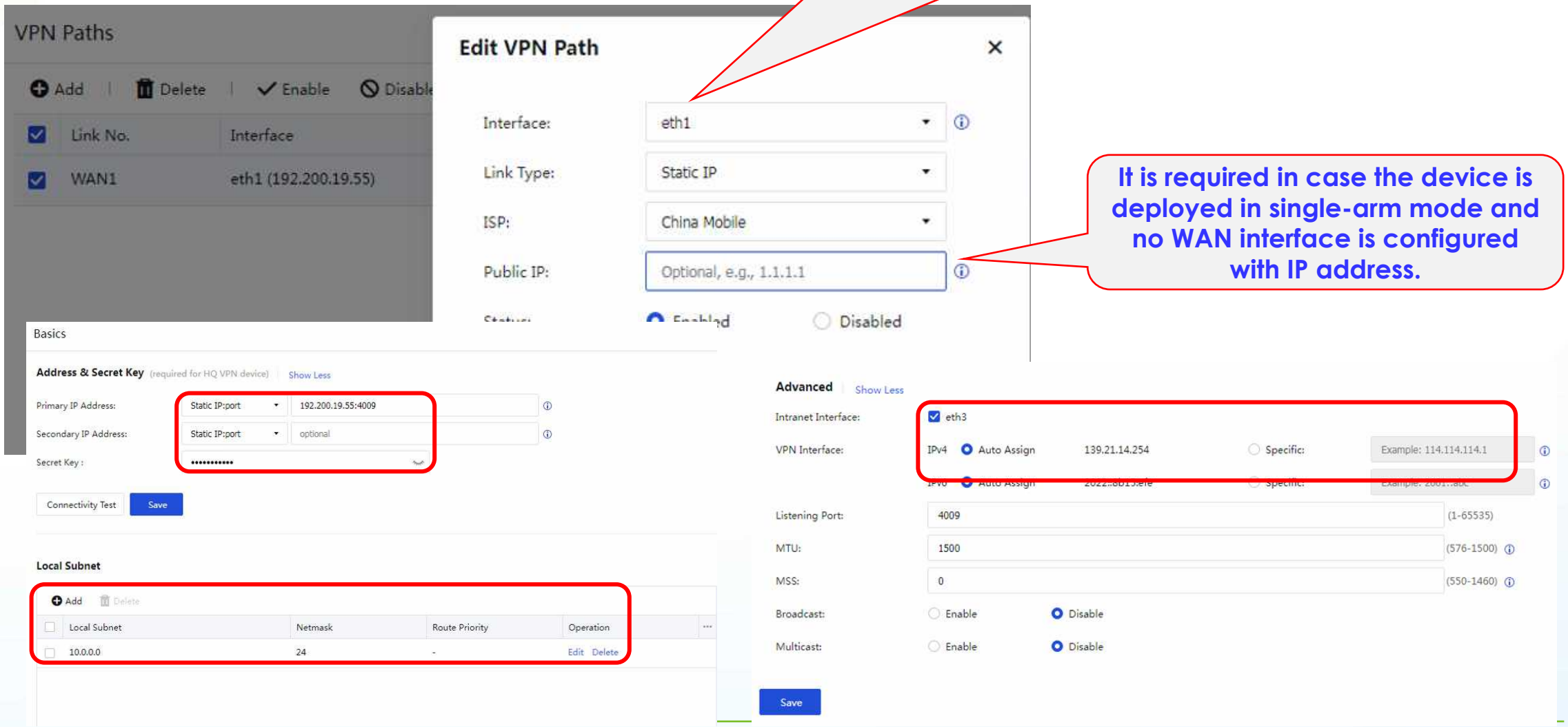
(2) Branch: Just configure the connection management.

Sangfor VPN

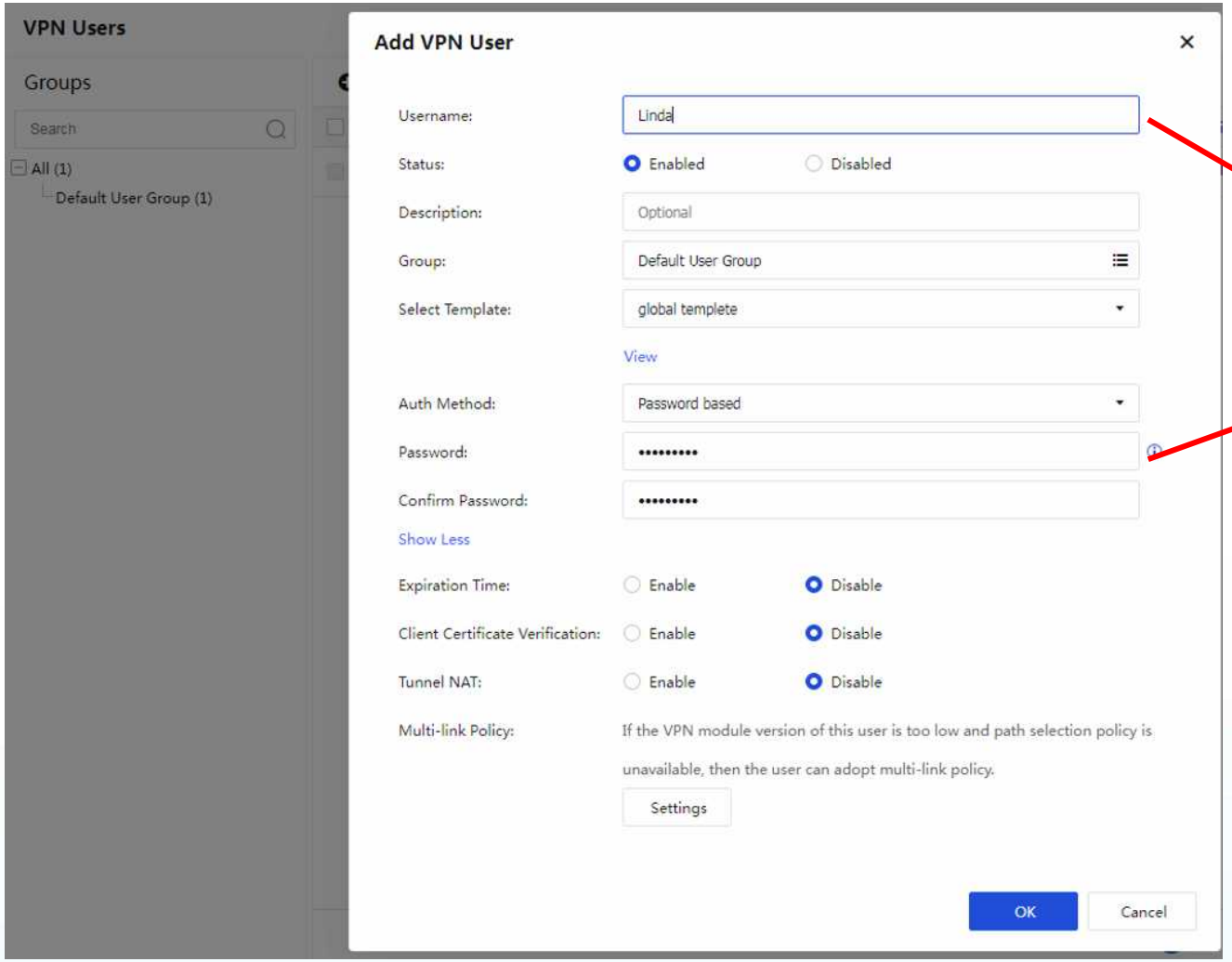
HQ Basic Settings

1. If there are no interfaces available, go to Network > Interface to configure a WAN interface.
2. If deployment mode is changed, delete the existing lines and add it again.

It is required in case the device is deployed in single-arm mode and no WAN interface is configured with IP address.



HQ Local Users setting

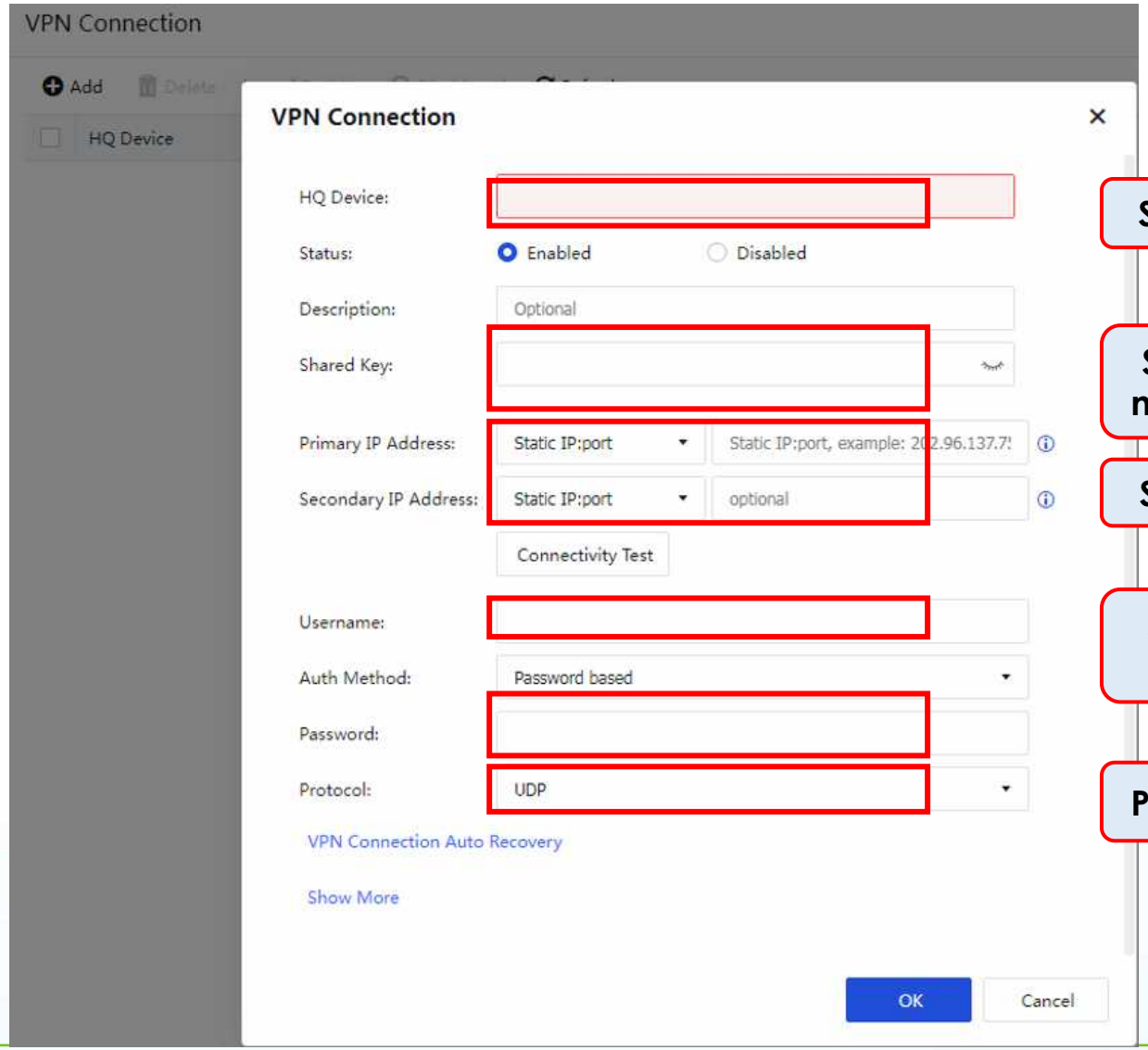


Set the Username and password for VPN authentication

Sangfor VPN

Branch setting:

VPN connection:



Set the peer name

Set the Shared Key, it must be same with HQ

Set the HQ webagent

Set the username and password

Protocol can be TCP or UDP

Sangfor VPN

	IPSec VPN	Sangfor VPN
Port	UDP 500,4500	Default TCP/UDP 4009; can modify
Tunnel NAT	No	Yes
Multi line support	No	Yes
Tunnel route	No	Yes
Tunnel service control	No	Yes
Tunnel traffic control	No	No
Multicast service	No	Yes
Static public IP	At least one	No
Company support	Most company	Only Sangfor

PART 3 SSL VPN

SSL VPN

SSL VPN for client VPN connection, making customer work convenient anywhere and anytime.

SSL VPN support:

Win XP, Win 7, Win 8, Win 10;

Linux Ubuntu 12.04.5,14.04.5, 14.04.6,17.04, 18.04.1

Linux Kylin v6.0, v7.0(64bits)

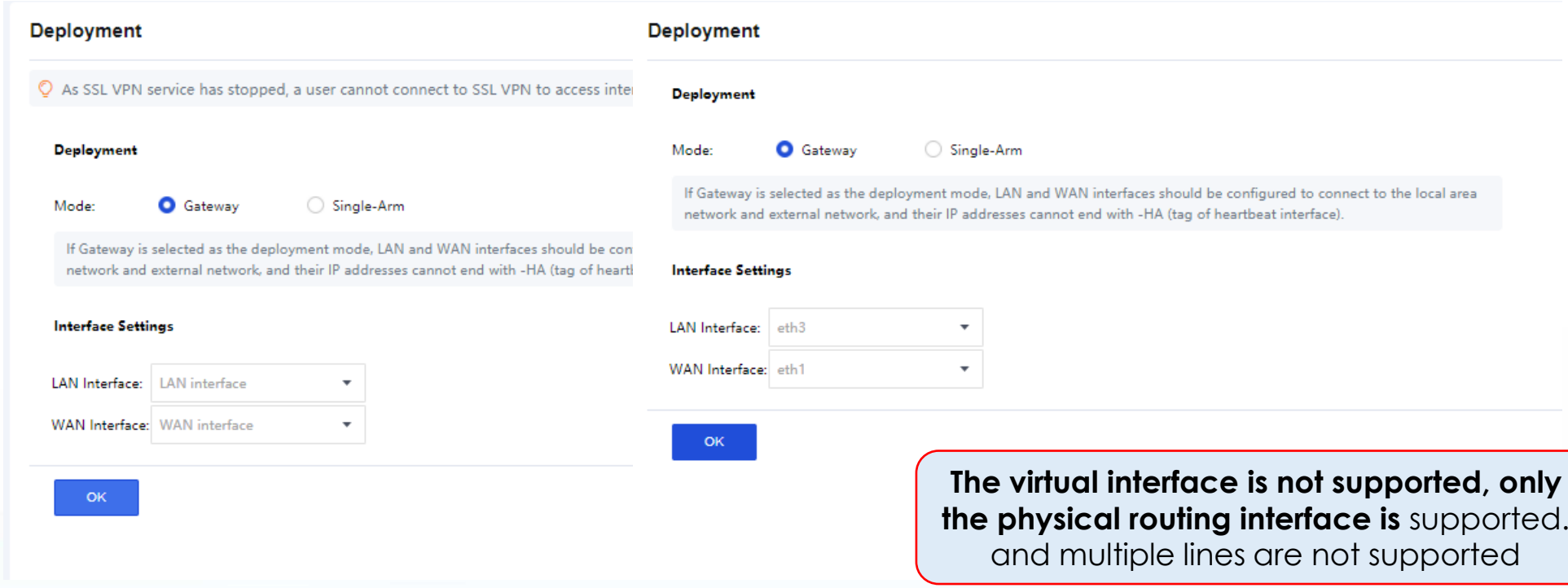
Mac OS 10.8/10.9/10.10/10.11/10.12/10.13/10.14/10.15;

Android 4.0 and later versions;

IOS 9 and later versions; (Need to download a software called Easy Connect from APP Store)

SSL VPN setting:

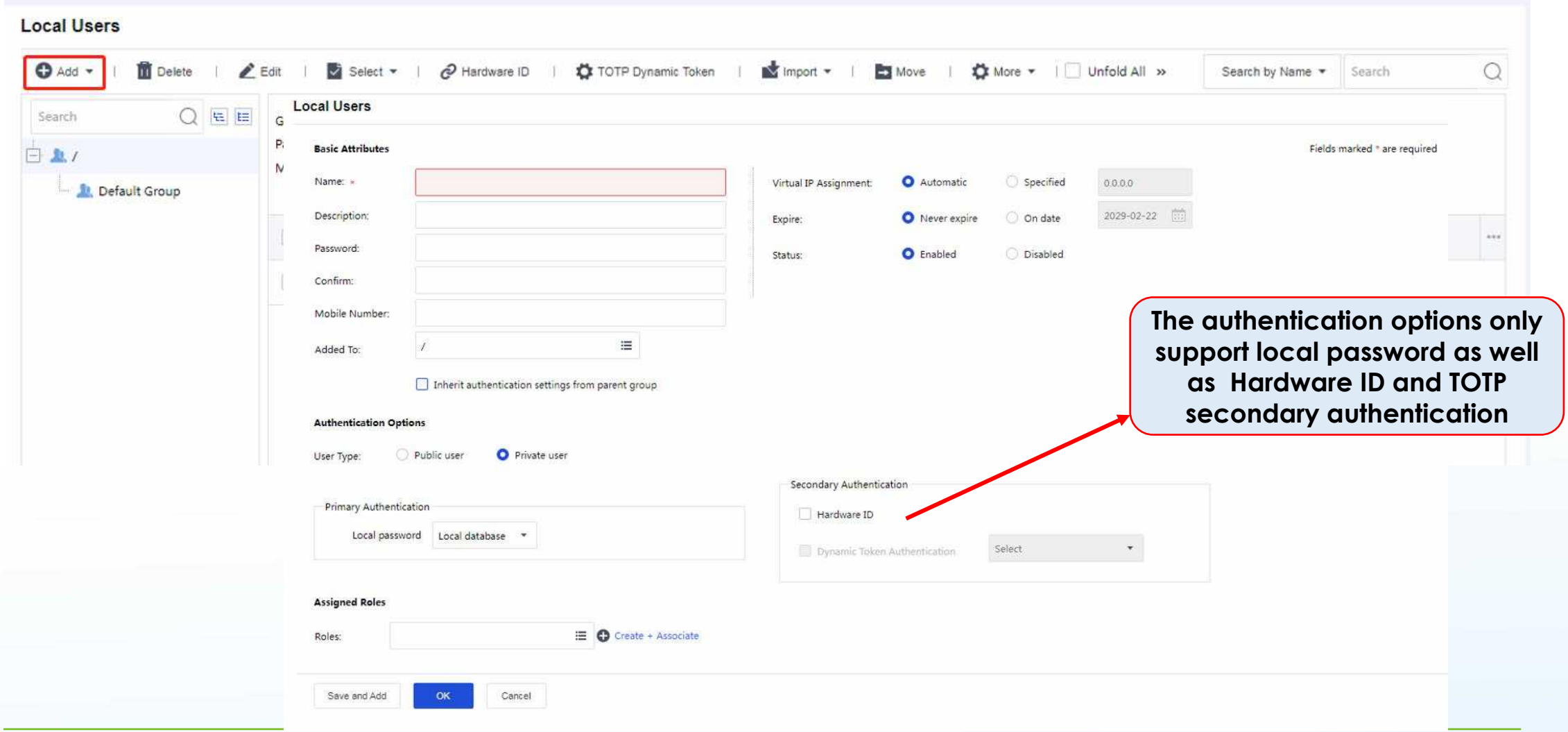
SSL Deployment, go to **Network > SSL VPN > Deployment. Before you configure the deployment , you will need to start the SSL VPN service**:



The virtual interface is not supported, only the physical routing interface is supported. and multiple lines are not supported

SSL VPN

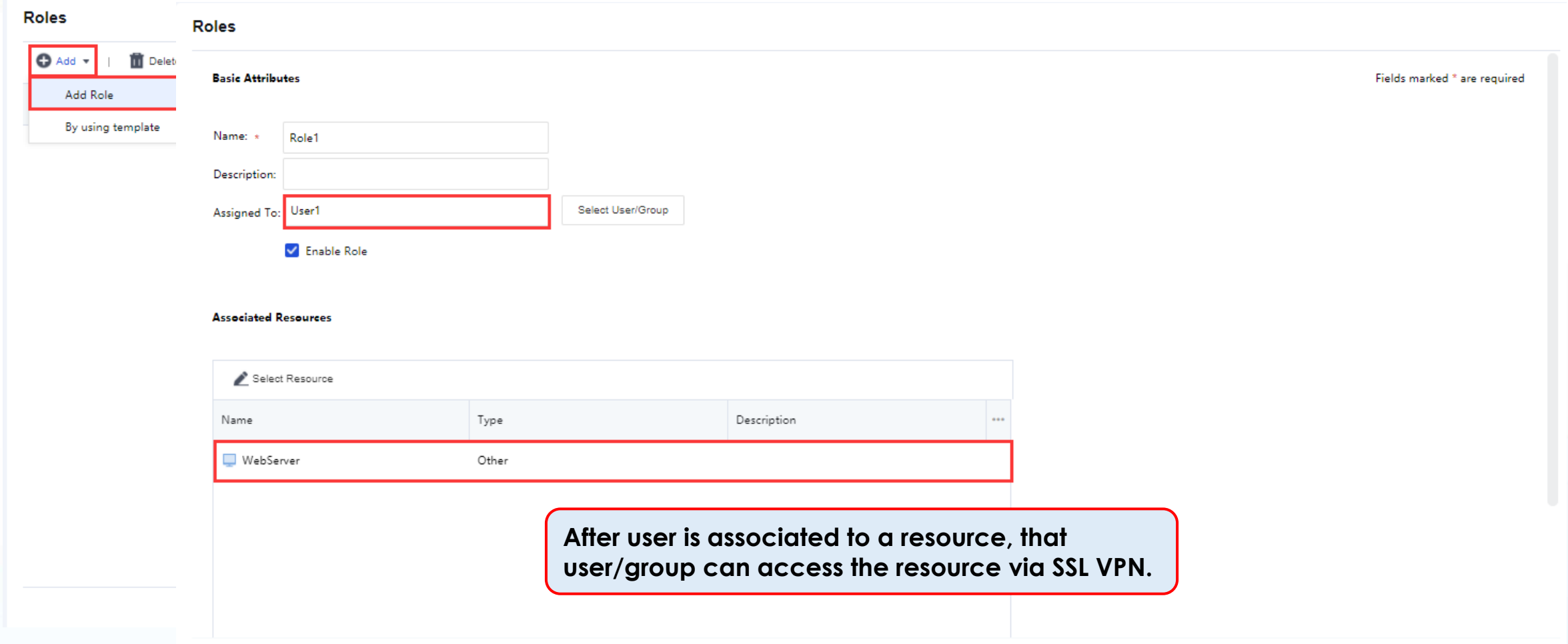
Users management:



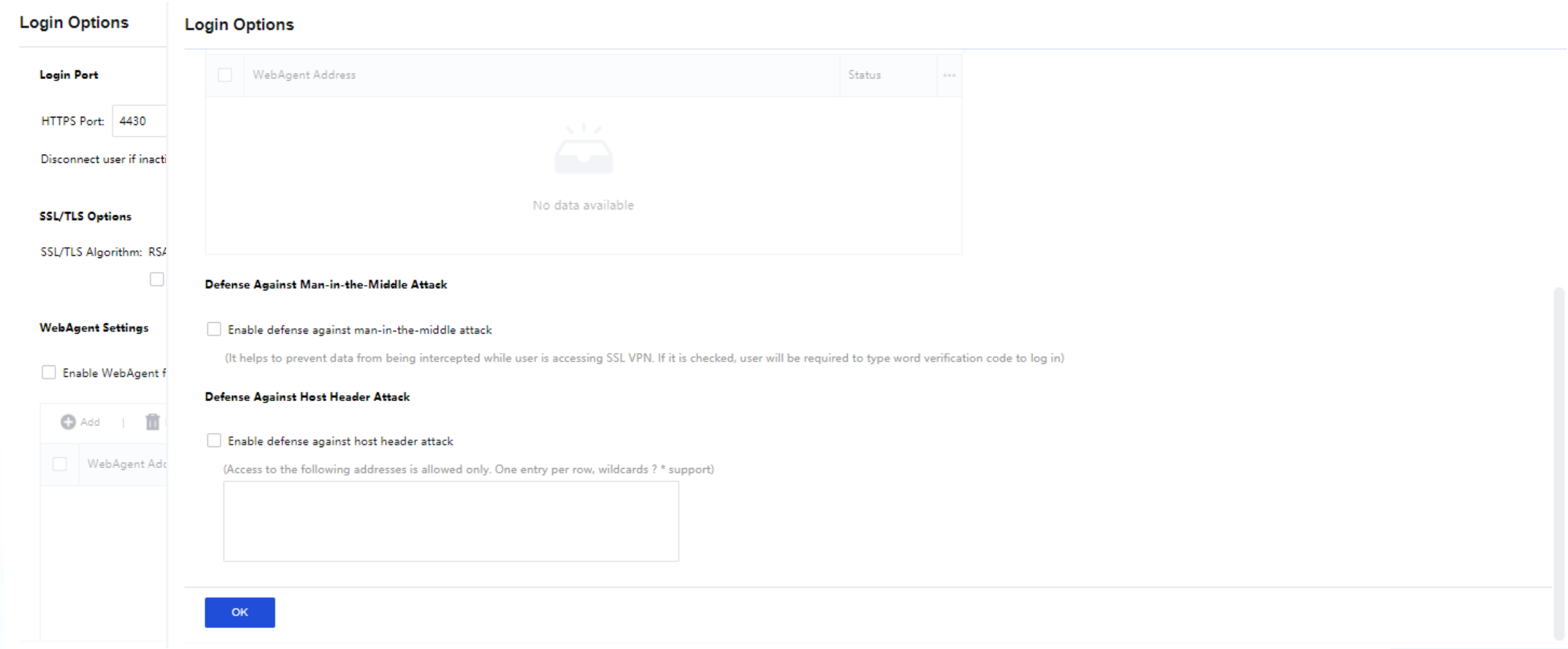
SANGFOR

Resources:

Roles:

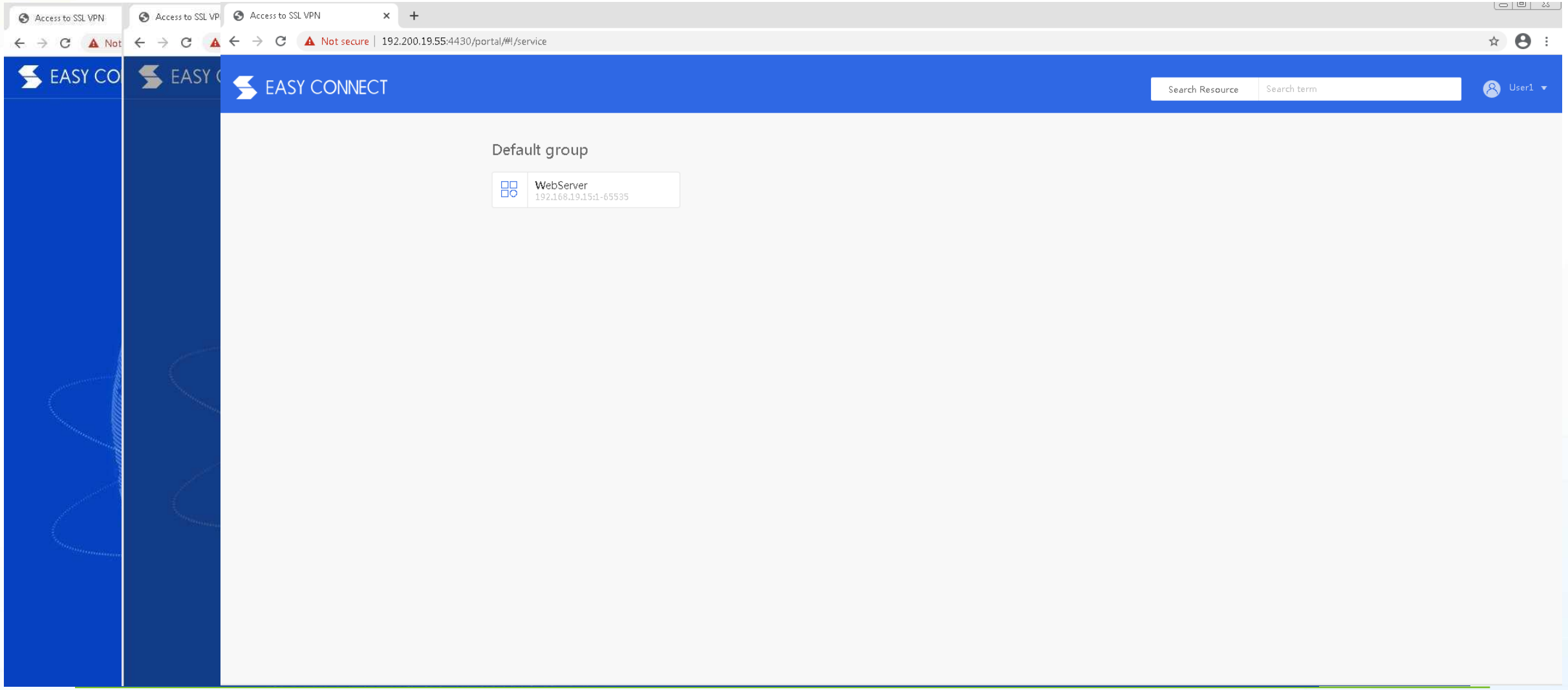

Roles
Add
Delet
Add Role
By using template
Roles
Basic Attributes
Fields marked * are required
Name: *
Role1
Description:
Assigned To:
User1
Select User/Group
Enable Role
Associated Resources
Select Resource
Name
Type
Description
WebServer
Other
After user is associated to a resource, that user/group can access the resource via SSL VPN.

Login Options:



SSL VPN

Client access to SSL



SANGFOR

THANK YOU

Technical Support Service

Email: tech.support@sangfor.com

Community: community.sangfor.com